A UNIFIED THEORY OF KNOWING EXPOSURE: RECONCILING *KATZ* AND *CARPENTER*

LUIZA M. LEÃO*

The search doctrine has long been in a state of disarray. Fragmented into different sub-doctrines, Fourth Amendment standards of constitutional protection vary based on how the government acquires the information in question and on how courts define the search that occurred. As trespass-based searches, reasonable expectation of privacy searches, consent-based searches, third-party searches, and private searches each trigger different levels of protection, the doctrine has become what more than one Justice has termed a "crazy quilt." This Note argues that unriddling the Fourth Amendment is easier than it might appear with the aid of the concept of knowing exposure, first discussed in Katz v. United States*. An undercurrent across different strands of the search doctrine, the knowing exposure principle holds that what one "knowingly exposes to the public" is beyond the scope of Fourth Amendment protection. As the Court grapples with the search doctrine in an age of unprecedented exposure to third parties, most recently in* Carpenter v. United States*, it should seek to unify the standard for searches around the foundational question of what renders one's exposure "knowing." Turning to* Carpenter*'s modifications to the third-party doctrine, this Note suggests a unified theory of knowing exposure that can apply across different kinds of searches, centering on whether the exposure is (1) knowing, (2) voluntary, and (3) reasonable.*

 J.D. 2022, New York University School of Law. I have great listeners to thank for this Note: Professors Barry Friedman and Erin Murphy, who guided me through the maze of the search doctrine; James Janison, for listening to my rants about legal wrongs; Joe Krakoff, for excellent suggestions; Yonas Asfaw-Cooper, Rupali Srivastava, David Blitzer, Sara Miller, Thomas Hislop, and Aadi Tolappa for great editorial comments; and Thomas Nielsen, for making this Note (and my whole life) wonderfully better. Thank you also to the *New York University Law Review* editorial team: Clare Platt, David Gross, Eliza Hopkins, and Ben Shand.

INTRODUCTION

The Fourth Amendment's search doctrine conundrum can be summarized neatly in a meme that has been circling the internet: A woman in a black and white picture grasps a telephone with an expression of horror. A caption reads: *People in the sixties: I better not say that or the government will wiretap my house*. Below her, a woman cooks next to an Alexa listening device, to which the woman asks: *Hey wiretap, do you have a recipe for pancakes?*[1] This is the amusing paradox of the modern search doctrine: While the Supreme Court has long held that one has no reasonable expectation of privacy in what one knowingly exposes to others, we currently expose the most intimate details of our lives to big tech corporations.[2] This development begs the overhauling of the third-party doctrine, which allows that information shared with third parties—like informants, banks, or Alexas—is accessible by the government.[3] Such information sharing, the doctrine currently holds, falls entirely outside the scope of a

[1] *See, e.g.*, *Hey Wiretap*, 9GAG (Nov. 16, 2017), https://9gag.com/gag/a3MzOb5 [https://perma.cc/BU7Z-R9KB].

[2] *See* Jack Nicas, *What Data About You Can the Government Get from Big Tech?*, N.Y. TIMES (June 14, 2021), https://www.nytimes.com/2021/06/14/technology/personal-data-apple-google-facebook.html [https://perma.cc/QF9L-348N] (reporting that "tech companies . . . often have access to the contents of their users' emails, text messages, call logs, photos, videos, documents, contact lists and calendars" and that most of this data "is available to law enforcement"); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2261–62 (2018) (Gorsuch, J., dissenting) ("What's left of the Fourth Amendment? Today we use the Internet to do most everything."); United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (commenting on the need to "reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties" especially during 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").

[3] On the extent to which this process happens, see generally Nicas, *supra* note 2.

Fourth Amendment search because one has no expectation of privacy (even from the government) in what one shares with third parties.[4]

As Justice Sotomayor has remarked, part of the problem is that the search doctrine has come to "treat secrecy as a prerequisite for privacy."[5] The Supreme Court has thus measured "knowing exposure" based on whether others have *access* to the information in question—be it through a transparent roof, a crack in the wall, the act of sharing our financial information with a bank, or of leaving our trash on the sidewalk to be rummaged by strangers.[6] But in reality, we have ceased to be secretive about the most intimate moments of our lives: We share our thoughts in text messages to cellphone service providers and software corporations, loan our faces to Instagram filters, and conduct our transactions via emails accessible by huge corporations. Below the body of those emails, however, those of us who are lawyers still write "privileged and confidential." Just because someone is *able* to access our information, it does not follow that we expect or entitle such access.

The constitutional search doctrine, however, insists that we behave secretively to enjoy Fourth Amendment protection. Original protection was tied to enumerated areas in the Constitution's text, so that the Supreme Court defined a search based on trespass into the home or other enumerated physical spaces. Eventually, the Court recognized that a search occurs whenever the government violates a "reasonable expectation of privacy."[7] To define this expectation, the Court has historically turned to a variety of tests and doctrines that are often irreconcilable.[8] A cardinal principle has been constant across different variations of the search doctrine, however: that what a person knowingly exposes to the public is not protected by the Constitution.[9] This principle assumes that it is not reasonable for the Court to protect you from governmental intrusion when you did not even try to protect yourself. People who leave their shades open,[10] walk or drive on public streets,[11] or willingly share information with

---

4 Smith v. Maryland, 442 U.S. 735, 743–44 (1979); *see also Carpenter*, 138 S. Ct. at 2219 (2018) ("The third-party doctrine partly stems from the notion that an individual has a reduced expectation of privacy in information knowingly shared with another."); California v. Greenwood, 486 U.S. 35, 41 (1988) ("A person has no legitimate expectation of privacy in information he voluntarily turns over to third parties." (citation and internal quotation marks omitted)).

5 *Jones*, 565 U.S. at 417–18 (2012) (Sotomayor, J., concurring).

6 *See generally infra* Section II.A.

7 *See generally infra* Section I.A.

8 *See infra* Part II.

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

10 *See* United States v. York, 895 F.2d 1026, 1029 (5th Cir. 1990).

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

others[12] are thus not generally allowed to cry "search!" when the government gets ahold of that which they have knowingly exposed to the world. As the Ninth Circuit has remarked, the Fourth Amendment is not like "J.K. Rowling's Invisibility Cloak, creat[ing] at will a shield impenetrable to law enforcement view even in the most public places."[13] This understanding assumes that individuals assume the risk of broad exposure, regardless of the scope of their initial disclosure, and that this assumption of risk triggers no Fourth Amendment protections.[14]

Reconceiving the Fourth Amendment for the modern information age is no easy task. Scores of scholars and jurists have taken stabs at clarifying the search doctrine, particularly as the speed of technology renders legal standards increasingly murky.[15] In 2018, the Supreme Court could have overhauled its search doctrine jurisprudence in *Carpenter v. United States*, and abandoned the notion that one has no constitutional protection in what one "shares" with third parties.[16] The Court could not agree on how to do so, however, struggling to refine its secretiveness-based standards for searches in a world where nothing is secret anymore.[17]

Part of the problem is that, largely due to path-dependency and the fact-based development of Fourth Amendment doctrines, the search doctrine is splintered into several sub-doctrines. The original

---

12 *See generally infra* Section II.A.

13 United States v. Gonzalez, 328 F.3d 543, 548 (9th Cir. 2003).

14 *See* Carpenter v. United States, 138 S. Ct. 2206, 2263 (2018) (Gorsuch, J., dissenting) (describing these two rationales as the flawed justifications for the third-party doctrine).

15 *See generally* Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801 (2004) [hereinafter Kerr, *New Technologies*] (arguing that the fast and changing nature of technological effects on privacy renders sweeping legal rules and constitutionally-framed standards inadequate when it comes to the Fourth Amendment); Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 476, 478 (2011) (arguing that the Fourth Amendment operates in a model of equilibrium-adjustment, in which "the Supreme Court adjusts the scope of Fourth Amendment protection in response to new facts in order to restore the status quo level of protection"); Ronald J. Allen & Ross M. Rosenberg, *The Fourth Amendment and the Limits of Theory: Local Versus General Theoretical Knowledge*, 72 ST. JOHN'S L. REV. 1149, 1162 (2012) (attributing such lack of doctrinal cohesion to the fact that "[t]he world of the Fourth Amendment is not the world of mathematics and formal analysis; it is instead the world of rain forests and spontaneous growth").

16 *See generally Carpenter*, 138 S. Ct. 2206.

17 Chief Justice Roberts fashioned a new standard for carving out an exception to the third-party doctrine when "sweeping" surveillance is at issue, *id.* at 2215, which Justices Alito, *id.* at 2257, Thomas, *id.* at 2246, and Kennedy, *id.* at 2227, found ran afoul of the Court's precedent in *Katz v. United States*, and which Justice Gorsuch dismissed as a feeble attempt that resulted in leaving the third-party doctrine "on life support," *id.* at 2272. *See generally infra* notes 89–96.

trespass doctrine, which bases constitutional protection on common-law physical trespass principles, runs alongside the reasonable expectation doctrine, which has since *Katz v. United States* protected privacy interests regardless of trespass.[18] Third parties add another layer to these doctrines. Before *Katz*, the Court had established that because private actors are exempt from Fourth Amendment liability, whenever third parties hand the product of their intrusion to the government, the government has not conducted a search.[19] This rule, known as the private search doctrine, means that even where a third-party actor has unlawfully trespassed and handed information over to the government, the government can use such information in its own investigations without any Fourth Amendment violation.[20] Yet, parallel to the private search doctrine, the third-party doctrine (which descends from *Katz*) finds that one has no reasonable expectation of privacy in what one *voluntarily* turns over to third parties.[21] This higher threshold of voluntariness is not entirely consistent with the private search doctrine which predated the third-party doctrine, and which continues to operate. Finally, third-party conduct is treated differently in a third sub-doctrine, the consent-based exception, which applies a different standard when third parties consent to a government search on behalf of a subject.[22] If you are confused by these different strands of doctrine, you are not alone: Scholars have noted that these separate standards treat the government and third parties differently in distinct scenarios, and that the results are far from consistent.[23] Even Justices have pointed out that the Fourth Amendment resembles more a "crazy quilt" than a legal doctrine, with different patches stitched together into a seemingly incoherent whole.[24]

This doctrinal fragmentation has grown more difficult to ignore in an age where searches no longer occur with wires worn by police informants or with police officers using binoculars. Instead, modern searches are private and ubiquitous, cutting across different sub-doctrines: On a daily basis, technology providers ask for your consent

---

[18] *See generally infra* Part I.

[19] *See infra* notes 133–36.

[20] *See infra* notes 133–36.

[21] *See generally infra* Section II.B.

[22] *See generally infra* Section II.B.

[23] *See, e.g.*, Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 126–37 (2002) (noting inconsistencies across different applications of the search doctrine); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823 (2016) (arguing for a doctrine rooted in positive law rather than applications of rules that are "freestanding" and "fashioned by courts on the fly").

[24] Smith v. Maryland, 442 U.S. 735, 745 (1979); Carpenter v. United States, 138 S. Ct. 2206, 2261 (2018) (Alito, J., dissenting) (quoting *Smith*, 442 U.S. at 745).

to retrieve your location data, then hand it over to the government.[25] In *Carpenter*, the Supreme Court treated such a process like a third-party search, finding the data mining too sweeping to be considered voluntary.[26] Yet when Google reads people's emails and hands information over to the government, lower courts have characterized this intrusion as a private search, exempt from constitutional liability.[27] At the same time, most users have likely consented, in some form, to this kind of data collection by providers.[28] Can different standards really apply depending on how we characterize these cases—as consent searches, third-party searches, or private searches?

Fourth Amendment scholars are largely split on what to do about these different doctrines. Some, like Orin Kerr, have attempted to reconcile them, arguing that the third-party doctrine applies the same standard as the reasonable expectation of privacy test for *Katz* cases that do not involve third parties.[29] Others, such as Matthew Tokson, focus on key underlying principles, such as knowledge of exposure, to argue for a more unifying rule across doctrines.[30] Finally, other scholars have thrown their hands up and embraced the unevenness of the doctrine as an inevitability in a path-dependent, reactive area of the law.[31] This Note shuns such nihilism, building on Tokson's work to distill an underlying, common principle: knowing exposure. This Note will show that the knowing exposure principle, which *Katz* left undefined and which no court—or scholarship—has given its due attention, already operates in most of these sub-doctrines. It is the common thread in this crazy quilt and can reconcile these different scenarios under one unifying standard without unraveling the doctrine altogether.

The proposed unified standard for knowing exposure in third-party doctrine cases would inquire whether the exposure was (1) knowing, (2) voluntary, and (3) reasonable from an objective, societal standpoint. In this endeavor, this Note will proceed in three parts. Part I describes the current status of the search doctrine, emphasizing

---

[25] *See generally supra* note 2 and accompanying text (explaining the *Hey Wiretap* meme, a potential example of a cross-sub-doctrine search).

[26] *Carpenter*, 138 S. Ct. at 2223. See *infra* notes 89–97 and accompanying text for an in-depth discussion of this standard.

[27] See *infra* notes 141–48 for a discussion of these cases.

[28] *See generally infra* note 162 and accompanying text (discussing consent provided to service providers in their terms of service).

[29] *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009).

[30] *See generally* Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139 (2016) (exploring the concept of knowledge across various areas of the search doctrine).

[31] *See supra* notes 22–23 and accompanying text.

knowing exposure as an underlying principle. Part II then juxtaposes modern, positive iterations of the knowing exposure rule against the normative standard for consent-based searches. Part III borrows the normative version of knowing exposure to form a three-part test. It then applies this standard to key doctrinal decisions, demonstrating that such an approach allows us to update the doctrine without obliterating it. The Note concludes that the knowing exposure rule from *Katz* needs to be revisited in an age in which we often expose ourselves to larger forces unknowingly, unwillingly, and unreasonably.

I
KNOWING EXPOSURE: THE COMMON THREAD

The knowing exposure rule dates from *Katz v. United States*, which first extended Fourth Amendment protections to those in public.[32] Since then, the principle has featured in subsequent opinions along two main theories: First, that one has no reasonable expectation of privacy in what one knowingly exposes to the public; and second, that one has no reasonable expectation of privacy in what one knowingly shares with third parties.[33] Although both of these principles are adjacent, they are unified in their assumption that knowing exposure renders one's information free of constitutional protection—because those who expose themselves to others either have no privacy interest in such information, or assume the risk that society will have access to it.

A. A Brief History of the Knowing Exposure Rule

The concept of "privacy" was first mentioned by the Supreme Court in a now-famous dissent by Justice Brandeis in *Olmstead v. United States*.[34] *Olmstead* held that the wiretapping of residential telephones did not amount to a constitutional search in the absence of physical trespass.[35] Brandeis critiqued the Court's rigid emphasis on trespass, reminding the Court that "[s]ubtler and more far-reaching means of invading privacy have become available to the Government."[36] Such foresight was essential, Brandeis noted, in interpreting a Constitution, which forces us to contemplate not only what

---

[32] 389 U.S. 347 (1967).

[33] *See supra* notes 18–22 and accompanying text.

[34] 277 U.S. 438, 474 (1928).

[35] *Id.* at 473 (Brandeis, J., dissenting) ("[A] principle, to be vital, must be capable of wider application than the mischief which gave it birth.").

[36] *Id.*

"has been," but also "what may be" as technology and society evolve.[37]

Almost a century later, these words ring sharp and true. In an age of cellphone recording, Alexas, smart doorbells, GPS tracking, drones, and all forms of digital recording and camera devices, courts are being forced to retool the Fourth Amendment and adapt older notions of privacy to a world in which privacy is constantly being invaded.[38] Yet the search doctrine seems to be in a perpetual state of déjà vu. Just as the rise of surveillance techniques in the mid-twentieth century rendered Justice Brandeis's prescient objection in *Olmstead* increasingly obvious, we now again find ourselves urging the Court to adapt its standards and move away from trespass in its decisions.[39]

Scholars have noted that although Justice Brandeis "lost the battle in *Olmstead*," he eventually "won the war."[40] In a line of cases from the 1950s to the 1960s, the Court formally recognized that the Constitution contemplated "privacy" as a right—and that this right was tied to the Fourth Amendment.[41] *Katz v. United States* took it a step further, finding that this right exists beyond the walls of the home, and that people in public could nonetheless be engaged in private acts deserving constitutional protection.[42] Finding that a conversation in a public phonebooth *was* protected by the Fourth Amendment, the Court delivered the famous line *Katz* is known for: that "[t]he Fourth Amendment protects people, not places."[43]

Katz thus ostensibly unmoored the constitutional protection from the specific enumerated areas in the text, decisively stating the intent

---

[37] *Id.*

[38] *See generally* Grant Clauser, *Security Cameras, Ethics and the Law*, N.Y. TIMES (Sept. 23, 2016), https://www.nytimes.com/wirecutter/blog/security-cameras-ethics-and-the-law [https://perma.cc/P696-GBD2] (describing the dilemmas posed by home Wi-Fi security cameras, an increasingly common tool for homeowners).

[39] *See* United States v. Jones, 565 U.S. 400 (2012) (relying on trespass to rule a GPS search unconstitutional); David C. Roth, Florida v. Jardines*: Trespassing on the Reasonable Expectation of Privacy*, 91 DENV. U. L. REV. 551, 553 (2014) (critiquing the Court's strict reliance on property law in *Florida v. Jardines*).

[40] RONALD JAY ALLEN, WILLIAM J. STUNZ, JOSEPH L. HOFFMAN, DEBRA A. LIVINGSTON & ANDREW D. LEIPOLD, CRIMINAL PROCEDURE: INVESTIGATION AND RIGHT TO COUNSEL 305 (2d ed. 2011).

[41] *See* Wolf v. Colorado, 338 U.S. 25, 27 (1949) ("The security of one's privacy against arbitrary intrusion by the police . . . is at the core of the Fourth Amendment."); Mapp v. Ohio, 367 U.S. 643, 660 (1961) (applying the exclusionary rule to the states and tying it to the recognition that "the right to privacy [is] embodied in the Fourth Amendment"); Griswold v. Connecticut, 381 U.S. 479, 485 (1965) (finding "the Fourth Amendment as creating a 'right to privacy, no less important than any other right carefully and particularly reserved to the people'" (quoting *Mapp*, 367 U.S. 643, 656)).

[42] 389 U.S. 347, 351–52 (1967).

[43] *Id.* at 351.

to separate the Fourth Amendment from trespass.[44] The decision also emphasizes the subjective perspective of the one seeking to retain his privacy: Rather than the physical boundaries of enumerated areas, it is what a person "seeks to preserve as private, even in an area accessible to the public," that confers constitutional protection.[45] This understanding has since been construed as the notion that it is an individual's "reasonable *expectation* of privacy" that determines whether such privacy exists, regardless of physical trespass or the intangible nature of the guarded object.[46]

But right after its famous sentence, *Katz* added an understated caveat: "*What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection*."[47] This knowing exposure asterisk has rendered *Katz* a difficult paradox: In freeing us from trespass, the decision built the search doctrine a new prison. The apparatus of surveillance technology which permeates our world is now free from Fourth Amendment scrutiny because the Court requires individuals to shield themselves from surveillance by choosing not to expose their movements and information to the public. This rationale places the burden of privacy on individuals seeking to retain it: One must be actively *seeking* to preserve one's privacy in order to claim constitutional protection. The Court has, with *Katz*'s blessing, come to hold that one has, it turns out, no reasonable expectation of privacy in one's disposed trash or in the interior of one's home that's visible from a police helicopter, or in the movements of one's cars on public streets.[48] Justice Brandeis's victory was, if anything, a pyrrhic one.

Katz's majority opinion did not tell us how to distinguish between someone knowingly exposing his deeds to the public and someone seeking to preserve them as private. In applying its own test, *Katz* looked to the physical attributes of the phonebooth in question, finding that just because Katz exposed himself visually by being in a glass booth, this did not mean he was expecting his private conversation to be overheard.[49] Justice Stewart's distinction between the "eye"

---

[44] *Id.* at 353.

[45] *Id.* at 351.

[46] *Id.* at 360 (Harlan, J., concurring) (emphasis added).

[47] *Id.* at 351 (emphasis added).

[48] *See* California v. Greenwood, 486 U.S. 35, 37 (1988) (no privacy interest in disposed trash); California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (no privacy interest in visible interior of home); United States v. Knotts, 460 U.S. 276, 281 (1983) (no privacy interest in car movements on public roads).

[49] *Katz*, 389 U.S. at 352; *see also* Edmund W. Kitch, Katz v. United States*: The Limits of the Fourth Amendment*, 1968 SUP. CT. REV. 133, 140 ("Would the case have been different if the pay phone had not been surrounded by a booth?").

and the "ear"[50] indicates that *Katz* emphasizes the individual's subjective expectation. It is whether one knows whether one is exposed that matters: One who knows that they are in a glass phone booth understands that the glass is see-through but also reasonably expects phone lines to be private. But the Court never explicitly addressed what made Katz's exposure to wiretapping "unknowing" enough to merit constitutional protection.[51]

One result of *Katz*'s lack of clarity on the knowing exposure standard was that subsequent decisions turned to other workable tests. One such alternative is the reasonable expectation of privacy test, proclaimed by Justice Harlan in his concurrence in *Katz*.[52] A second standard is the one developed by Justice White's concurrence: the notion that assumption of risk principles operate in surveillance cases, which originally borrowed from pre-*Katz* decisions and has since evolved into the oft-challenged third-party doctrine.[53] Though the Supreme Court rarely discusses "knowing exposure" when applying these search doctrine frameworks, the concept of knowing exposure has operated as a dormant principle in these lines of jurisprudence.

B. Knowing Exposure as Access: The Reasonable Expectation of Privacy Test

Justice Harlan's reasonable expectation of privacy test, now the main takeaway from *Katz*, enumerates two prongs for determining whether one has a privacy interest protected by the Fourth Amendment.[54] A person thus has a reasonable expectation of privacy if they "*first*, . . . exhibited an actual (subjective) expectation of privacy and, *second*, . . . the expectation [is] one that society is prepared to recognize as reasonable."[55]

---

[50] *Katz*, 389 U.S. at 352.

[51] In fact, some have since noted that *Katz* was a third-party case. *See, e.g.*, Alex Kozinski & Eric S. Nguyen, *Has Technology Killed the Fourth Amendment?*, 2011–2012 CATO SUP. CT. REV. 15, 26 (2012) (asking, if *Katz* were decided today, "[w]ould the Court really say that a guy standing on a street corner shouting into his cell phone had a reasonable expectation of privacy?").

[52] *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

[53] *Id.* at 363, n.1 (White, J., concurring); *see also infra* Section II.A (discussing the third-party doctrine's evolution).

[54] *Id.* at 361 (Harlan, J., concurring). Justice Harlan was frank in his reinterpretation of *Katz*: "I join the opinion of the Court," he wrote, "which I read to hold only . . . that an enclosed telephone booth is an area where, like a home, and unlike a field, a person has a constitutionally protected reasonable expectation of privacy." *Id.* at 360; *see also* Smith v. Maryland, 442 U.S. 735, 740 (1979) (applying the two-part test from Harlan's concurrence); Carpenter v. United States, 138 S. Ct. 2206, 2237 (2018) (Thomas, J., dissenting) (noting that Harlan's test has since become the landmark *Katz* ruling because it at least "attempted to articulate the standard that was missing from the majority opinion").

[55] *Katz*, 389 U.S. at 361 (Harlan, J., concurring) (emphasis added).

The second prong of Justice Harlan's formula, however, has allowed physicality and enumeration to surreptitiously sneak back into the *Katz* test. For instance, courts have found that those whose deeds were visible by officers, even in open fields near their own homes, are not protected by the doctrine because, even if one had a subjective expectation of privacy, such an expectation is not one which society is "prepared to recognize as reasonable."[56] In *United States v. Knotts*, the Burger Court held that one has no expectation of privacy when driving about on public streets, so that the GPS tracking of a vehicle did not constitute a search.[57] Three years later, in *California v. Ciraolo*, the Court relied on Justice Harlan's rule to extend this rationale even into the home, finding that no search had occurred when the police used a plane to fly over a suspect's backyard to determine whether he was growing marijuana in a greenhouse.[58] Because the interior of the greenhouse was *visible* to the naked eye from an aerial perspective, and the officer's presence in the airplane was not unlawful, the onus was on the homeowner to hide his backyard from view, not on the police to "shield their eyes."[59]

The twist on the expectation of privacy doctrine is that, so long as a police officer is lawfully allowed to be where he is, anything within his perception is beyond the scope of the Fourth Amendment—even when his sensorial perception is aided by additional devices.[60] Usually, the measure of "secretiveness" is a physical one: the existence of a wall covering or rooftop, or whether a bag was opaque or transparent.[61] Thus, even in decisions in which courts have applied the rea-

---

[56] Oliver v. United States, 466 U.S. 170, 177, 181 (1984).

[57] 460 U.S. 276, 285 (1983).

[58] 476 U.S. 207, 213–14 (1986).

[59] *Id.* at 213. The Court ruled the same a few years later, when the police used a helicopter rather than a plane. Florida v. Riley, 488 U.S. 445, 450 (1989) ("The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.").

[60] *See* Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) ("The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems."); United States v. Jackson, 213 F.3d 1269, 1281 (10th Cir. 2000) (holding that cameras installed on telephone poles capture "only what any passerby would easily have been able to observe"), *vacated on other grounds*, 531 U.S. 1033 (2000).

[61] *See* California v. Ciraolo, 476 U.S. 207, 213–14 (1986) (noting that since the defendant's rooftop had transparent tiles, "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed"); Oliver v. United States, 466 U.S. 170, 179 (1984) (holding that no search occurred where police trespassed onto defendant's yard because "fences or 'No Trespassing' signs do not effectively bar the public from viewing open fields"); Robbins v. California, 453 U.S. 420, 426 (1981) (emphasizing that the contents of a "closed, opaque container" are worthy of Fourth Amendment protection because those contents "would remain free from public examination").

sonable expectation of privacy test, physical elements have continued to feature significantly in the construction of what constitutes a "reasonable" expectation, so that if there is no physical barrier shielding the eye of a policeman, for instance, such an expectation is not considered a reasonable one. Yet *Katz* held that what one "seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected."[62] The emphasis should therefore be on whether one is *seeking* to preserve something as private—a question most courts elide by focusing on whether the actual object of the search was lawfully accessible to the public.[63]

The current approach thus conflates expectation of privacy with access. As the Court noted in *Ciraolo*, the government's mode of observation is analogous to "a knothole or opening in a fence: if there is an opening, the police may look."[64] In treating such access as a proxy for knowing exposure, the Supreme Court has left the Fourth Amendment vulnerable to access-enhancing technologies. Just as an officer could with the aid of a camera or helicopter access viewpoints that would render a subject's activities visible and thus exposed, so too now can the police lawfully access a wide span of activity happening in the public streets by having drones fly overhead. Similarly, if you tell a secret to an undercover informant who transmits your voice to the police through concealed wires, the police's ears have lawful access to your words, which you have knowingly exposed to them—even if you did not know their ears were listening in.[65]

Acknowledging these loopholes in the reasonable expectation of privacy approach, the Supreme Court has returned to trespass time and again.[66] In *Jones v. United States*, the Court found that attaching a GPS tracking device to a car without a warrant was an unconstitutional search because the act of installing the tracking device

---

62 Katz v. United States, 389 U.S. 347, 351–52 (1967).

63 *See* Minnesota v. Dickerson, 508 U.S. 366, 374–75 (1993) (expounding on the plain view doctrine).

64 *Ciraolo*, 476 U.S. at 210.

65 *See* United States v. White, 401 U.S. 745, 751(1971) (holding that there is no reasonable expectation of privacy in conversations with others and, therefore, the Fourth Amendment does not bar government agents from testifying to what they heard over a wiretap worn by an informant).

66 A notable exception was the Court's decision in *Kyllo v. United States*, where Justice Scalia devised a three-prong test for intrusive technologies under the reasonable expectation of privacy framework: (1) sense-enhancing technology revealing information on the interior of a home that (2) could not otherwise have been obtained without physical intrusion into a constitutionally protected area constitutes a search, at least (3) if such technology "is not in general public use." 533 U.S. 27, 34 (2001). No subsequent Court decision has since applied this test, however, and two Scalia opinions—*United States v. Jones*, 565 U.S. 400 (2012), and *United States v. Jardines*, 569 U.S. 1 (2013)—have since opted for returning to the trespass framework.

amounted to a trespass.[67] The *Katz* reasonable expectation test, reasoned the majority, merely "*added to*, [rather than] *substituted* . . . the common-law trespassory test," which could easily be applied whenever enumerated areas were at issue.[68] In the modern information age, it seems nonsensical—as the dissenting and concurring opinions noted—to base whether a search occurred on the fact that a tracking device touched a car.[69] But the majority had its reasons to dismiss discussions of privacy expectations: By driving his car on a public road, Jones had "knowingly exposed" himself to observation—and thus did not have any expectation of privacy in his vehicle's movements, as the Court had ruled decades earlier.[70] Another example of this stretching of trespass to avoid the gutted *Katz* test is *Florida v. Jardines*. There, the Court held that police violated the Fourth Amendment when they took a sniffing dog over a suspect's porch, because the porch was a constitutionally protected area and the dog sniff therefore amounted to a trespass.[71] Justice Kagan, in her concurrence, was adamant that the case could be decided on "privacy as well as property grounds," comparing it to the analogy of a stranger at the front door of your home "carrying super-high-powered binoculars."[72] Yet the majority decided the case strictly on property grounds, emphasizing the physical elements of the case.[73]

This modern trespass approach has left Justices debating how long dogs have been domesticated in the United States,[74] or whether a constable could have hidden in an eighteenth-century coach undetected and functioned like a GPS tracking device.[75] But while focusing on physical intrusion loses the forest for the trees, the modern reasonable expectation of privacy approach loses the forest *and* the trees. By emphasizing ease of access—regardless of whether such access was predictable, anticipated, invited, or normatively consistent with privacy expectations—the modern *Katz* doctrine has left us barely any

---

[67] *Jones*, 565 U.S. 400, 404 (2012).

[68] *Id.* at 409.

[69] *Id.* at 419 (Alito, J., dissenting) (chastising the majority's decision as "highly artificial"); *id.* at 414 (Sotomayor, J., concurring) ("Nonetheless, as Justice Alito notes, physical intrusion is now unnecessary to many forms of surveillance.").

[70] United States v. Knotts, 460 U.S. 276, 281 (1983).

[71] Florida v. Jardines, 569 U.S. 1, 4–6 (2013).

[72] *Id.* at 12 (Kagan, J., concurring).

[73] *Id.* at 11.

[74] *See id.* at 16–17 (Alito, J., dissenting).

[75] *See* United States v. Jones, 565 U.S. 400, 406 n.3 (2012) (justifying an originalist approach to the case at bar because its situation is similar to "a constable's concealing himself in the target's coach in order to track its movements"); *id.* at 420 & n.3 (Alito, J., concurring) ("[T]his would have required either a gigantic coach [or] a very tiny constable.").

protection, both in public and at home, when it comes to big tech and government surveillance. As courts have expanded the concept of public access into the virtual dimension, they now assume that if you share some information with a third party, you are knowingly sharing information with anyone that party wishes to disclose it to—including the government.[76]

Katz's lack of definition of its knowing exposure standard has, in sum, engendered a redoubled emphasis on physicality in a legal field that increasingly deals in intangibles, whether the court follows the trespass framework or the reasonable expectations of privacy approach. After all, the modern *Katz* formulation assesses whether outsiders have *access* to the information being surveyed, looking to what *is*—I *can see* intimate details of your life through your window, or read your text messages—to determine what *should be*. This framework gives us no normative standards for Fourth Amendment protection, and ultimately ignores the provision's purposes, replacing them with the haphazard way in which we have given up the right it endows.[77] Its current status flies in the face of Justice Stewart's reminder to the Court a few years after *Katz*: "If times have changed, reducing everyman's scope to do as he pleases in an urban and industrial world, the changes have made the values served by the Fourth Amendment more, not less, important."[78]

As Part II of this Note will illustrate, this positive emphasis on what people in actuality *do* in order to define the normative scope of constitutional rights takes its most concerning form when it comes to the third-party doctrine. Yet the knowing exposure rule from *Katz* does not have to be positive. In fact, the search doctrine already has defined normative standards for when third-party actors unreasonably consent to searches: Assumption of risk and consent are two conceptual justifications for the absence of Fourth Amendment protections. As *Carpenter* has forced lower courts to confront the inconsistencies between these different approaches when the private-search doctrine and the third-party doctrine overlap, these two versions of the third-party doctrine allow us to return to first principles. This Note argues that the overarching, silent norm that underlies these different strands of the search doctrine is an undefined knowing exposure standard.

---

[76] *See generally infra* Section II.B.

[77] For a sharp critique of this result, see Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 161 (2008) (noting that the Fourth Amendment's "central purpose, to protect the people's right to be secure, has been lost, supplanted by an effort to protect individuals' expectations of privacy").

[78] Coolidge v. New Hampshire, 403 U.S. 443, 455 (1971).

II
Access Versus Consent: A Tale of Three Third-Party Doctrines

One of the fruits of the *Katz* test is the third-party doctrine, which holds that "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[79] As currently framed, this rule expands on the notion of knowing exposure as access, defining "third party" broadly to include individuals to whom you tell your secrets,[80] your bank,[81] and your cellphone company.[82] A kernel of the doctrine might make sense: It is fair for the government to assume that what you go around telling people is not something over which you expect privacy. But the rule has expanded miles around this kernel, allowing the government to outsource Fourth Amendment searches to private actors while eschewing constitutional liability.[83] It also is difficult to reconcile with the private-search doctrine, which holds that the Fourth Amendment does not apply to searches conducted by third parties, even if their actions were blatantly unlawful, or when the contents of these searches are later turned over to the government.[84] Both of these doctrines are positively, rather than normatively, constructed. Yet interwoven awkwardly in between them lies an interesting alternative: the consent-based version of the third-party doctrine, which establishes normative boundaries for the intrusion of third-party searches.

As technology has caused many to rethink the precarious logic of the third-party doctrine,[85] the Supreme Court has recently begun to question its scope.[86] And for good reason. After all, it rests on two faulty premises: first, that by exposing ourselves to one individual, we have exposed ourselves to the world at large; and second, that we willingly expose ourselves (and assume the risk of intrusion) in scenarios where we had little choice but to turn over our information to third-party agents, such as opening a bank account or purchasing a tele-

---

[79] Smith v. Maryland, 442 U.S. 735, 743–44 (1979).

[80] *See generally* United States v. White, 401 U.S. 745 (1971) (extending this rationale to wiretapped informants).

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

[82] *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018) (discussing whether this rationale extends to cell-site location information).

[83] *See supra* note 2 and accompanying text.

[84] *See infra* Section II.B.

[85] For commentators maligning the third-party doctrine, see generally Kerr, *supra* note 29, at 570 (compiling critiques of the doctrine).

[86] *See Carpenter*, 138 S. Ct. at 2224 (declining to extend the third-party doctrine to instances of sweeping surveillance); Riley v. California, 573 U.S. 373, 397–98 (2014) (discussing the heightened "privacy interests" of individuals in the contents of their cellphones).

phone. Sharing information with *one* party (be it your friend, phone provider or financial adviser) does not automatically mean you have knowingly shared it *with the public*.[87] Just because you have come to allow Google to read your emails does not mean you have also allowed Google to share their contents with law enforcement officers—and even holding that you have allowed Google access to this information in the first place might be a bit of a stretch.[88]

The Supreme Court last faced the third-party doctrine's pitfalls in *Carpenter v. United States*, in which Chief Justice Roberts carved out an exception to the doctrine based on its scope, rather than its fundamentals.[89] In *Carpenter*, the Court held that the doctrine did not apply to cell-site location information (CSLI) when the surveillance in question was sweeping, relying on four factors to reach this conclusion: (1) how revealing the information was; (2) the degree of exposure; (3) the aggregate effect of such surveillance on society; and (4) the inescapability of surveillance to invalidate the assumption of risk reasoning.[90] However, the majority insisted that its holding was narrow, applicable only to CSLI for the time being, and didn't disturb older third-party doctrine decisions.[91] Coupled with a lack of clear guidance on how to apply these four factors, *Carpenter* produces a puzzling result: How could CSLI surveillance be more sweeping than other forms of surveillance the Court has consistently upheld, like bank and phone records?[92] *Carpenter*'s carve-out for "sweeping" surveillance may have been necessary, but its logic leaves many questions unanswered.[93] Lower courts have struggled with the lines the ruling does not draw and have hesitated to apply this potentially game-changing

---

87 *See supra* Section I.B.

88 *See infra* Section II.B.

89 *See Carpenter*, 138 S. Ct. at 2220 (explaining that *Carpenter*'s holding does not disturb the holdings in *Smith* and *Miller*).

90 *Id.* at 2223 ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection."); *see also* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 370 (2019) (narrowing the list to three factors).

91 *Carpenter*, 138 S. Ct. at 2220 ("Our decision today is a narrow one. . . . We do not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques and tools, such as security cameras. Nor do we address other business records that might incidentally reveal location information.").

92 *See id.* at 2272 (Gorsuch, J., dissenting).

93 *See id.* at 2220 n.4 ("[W]e 'do not begin to claim all the answers today,' . . . and therefore decide no more than the case before us." (citation omitted)); *see also* Ohm, *supra* note 90, at 366 (arguing that the narrow scope of *Carpenter* is somewhat inconsistent with the breadth of its principles).

exception to analogous scenarios.[94] It is, after all, important, wrote Justice Roberts, that the Court "tread carefully in such cases to ensure that we do not 'embarrass the future.'"[95]

As Justice Gorsuch highlighted in his *Carpenter* dissent, it makes little sense to keep the third-party doctrine on "life support"[96] when the rationales that underlie it ultimately are flawed. Two principles arguably underlie the third-party doctrine, assumption of risk and consent.[97] This Part looks to these two theories to argue that they can be reconciled with an overarching principle: knowing exposure. The first, the assumption of risk framework, iterates the positive, access-based version of reasonable expectation of privacy: the notion that if someone *can* or *does* have access to your information, you have assumed the risk that they will have that access, and thus abdicate your Fourth Amendment protections. The second approach to the third-party doctrine, however, operates on the basis of consent, emphasizing whether the third-party agent has the authority and legitimate control over the information to consent to its inspection on your behalf. This framework, seen in consent exception cases in the 1970s and 1980s, considers whether the third party has overreached by conducting a search of your private affairs.

A. Exposure as Access: The Third-Party Doctrine as Assumption of Risk

The third-party doctrine was fully articulated in *Smith v. Maryland*, in which the Court held that one has no privacy expectations in their phone records.[98] There, the police used a pen register to record the numbers that Smith had dialed on his home telephone. Such activity was not a search, the Court concluded, because "even if petitioner did harbor some subjective expectation that the phone numbers he dialed would remain private, this expectation is not 'one that society is prepared to recognize as "reasonable."'"[99] This expec-

---

[94] *See generally* Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1791 (2022) (compiling lower court decisions since *Carpenter* and noting that the decision was "notoriously vague," so that "[s]cholars and lower courts have tried to guess at what the law of Fourth Amendment searches will be going forward—and have reached different, contradictory conclusions").

[95] *Carpenter*, 138 S. Ct. at 2220 (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

[96] *Id.* at 2272 (Gorsuch, J., dissenting).

[97] *See id.* at 2263.

[98] *See* 442 U.S. 735, 742 (1979) (rejecting the petitioner's argument that he had a "'legitimate expectation of privacy' regarding the numbers he dialed on his phone").

[99] *Id.* at 743 (quoting Katz v. United States, 389 U.S. 347, 361 (1967)).

tation is not reasonable, the majority ruled, because "a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."[100] The third-party doctrine is thus a child of Justice Harlan's reasonable expectation test: One has no Fourth Amendment protection in what one turns over to third parties because such an expectation is not one the Court considers objectively reasonable.[101]

Embedded in the third-party doctrine, then, is the same assumption of risk rationale that guides the reasonable expectation of privacy test: Just as one who leaves their blinds open assumes the risk of peeping toms, one who divulges secrets to a third party assumes the risk of the government recording their statements.[102] Justice White first articulated this reasoning in his concurrence in *Katz*, writing that a person in conversation assumes "the risk that the man to whom he speaks will make public what he has heard," and recording and transmitting devices fall within this familiar category of risk-taking.[103] Like Justice Harlan, Justice White was working with what he had. Looking to previous surveillance decisions, his reading of *Katz* sought to reconcile the majority's opinion with existing decisions it assumed *Katz* had not overruled.[104]

Subsequent decisions, however, never paused to ponder whether this assumption of risk principle was indeed what "knowing exposure" meant. Just like Justice Harlan's emphasis on lawful access, this framework is positive rather than normative: It supposes that if I *can* see what's in your bag, then I have the right to see it, since, by making your bag vulnerable to my sight, you assumed the risk that I would look in.[105] This assumption makes it your job, rather than the Constitution's, to conceal from me what you wish to keep private. And if you fail to protect yourself, you have invited the world's eyes and ears, assuming the risk of having your private affairs seen, overheard, recorded, transmitted, or filmed not only by one person, but by the whole world.

---

[100] *Id.* at 743–44.

[101] *See supra* Part I.

[102] *See* United States v. White, 401 U.S. 745, 751–52 (1971) (explaining that a government agent's recording of their conversation with the defendant did not invade the defendant's "constitutionally justifiable expectations of privacy").

[103] *Katz*, 389 U.S. at 364 n.1 (1967) (White, J., concurring).

[104] *Id.* (noting that "[i]n previous cases, which are undisturbed by today's decision, the Court has upheld, as reasonable under the Fourth Amendment, admission at trial of evidence obtained" by undercover informants listening to conversations with transmission devices).

[105] *See supra* note 60 and accompanying text.

The assumption of risk principle became controlling in *United States v. White*, a case involving wired surveillance by an informant, when Justice White reasoned that "[i]nescapably, one contemplating illegal activities must realize and risk that his companions may be reporting to the police," and that "the risk is his," regardless of the manner in which this risk manifests.[106] Although support from other Justices on the bench for this view at the time was short of overwhelming,[107] this assumption of risk principle has since evolved into the third-party doctrine, which has come to reproduce Justice White's premise in a cadence of intensifying information-sharing in exchange for socio-technological benefits: One who opens a bank account assumes the risk that the bank will reveal their personal information to the government;[108] one using a telephone assumes the risk that the phone company will turn over records of numbers dialed;[109] one who owns a cellphone knowingly accepts the possibility that geolocation information may be subpoenaed from the service provider.[110]

The third-party doctrine is overt in its reliance on the knowing exposure principle. In *Smith*, the Court reasoned that "[w]hen he used his phone, petitioner voluntarily conveyed numerical information to the telephone company and '*exposed*' that information to its equipment in the ordinary course of business. In so doing, petitioner assumed the risk that the company would reveal to police the numbers he dialed."[111] As Orin Kerr has remarked, the third-party doctrine unifies the *Katz* reasonable expectation doctrine around this defining principle—just as you have knowingly exposed yourself in public to officers from a lawful vantage point, so too have you knowingly exposed yourself to a third party.[112]

---

106 *White*, 401 U.S. at 752. Justice White was also frank in his bias in favor of electronic surveillance as a way of capturing accurate evidence of criminal behavior. *See id.* at 753 ("Nor should we be too ready to erect constitutional barriers to relevant and probative evidence which is also accurate and reliable.").

107 *See id.* at 755–56 (Brennan, J., concurring) (concurring solely because the Court had previously held that *Katz* did not apply retroactively); *id.* at 756 (Douglas, J., dissenting) ("What the ancients knew as 'eavesdropping' we now call 'electronic surveillance'; but to equate the two is to treat man's first gunpowder on the same level as the nuclear bomb.").

108 *See* United States v. Miller, 425 U.S. 435, 443 (1976) (concluding there is no expectation of privacy in financial records held by a bank).

109 *See* Smith v. Maryland, 442 U.S. 735, 743 (1979) (concluding that there is no expectation that the numbers that telephone subscribers dial will remain confidential).

110 *See* Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018) (concluding that cellular geolocation data may be subpoenaed from a service provider).

111 *Smith*, 442 U.S. at 744 (emphasis added).

112 *See* Kerr, *supra* note 29, at 561 (arguing that the doctrine "matches the Fourth Amendment rules for information to the rules for location, creating clarity without the need for a complex framework of sui generis rules"). *But see* Colb, *supra* note 23, at

Yet while the element of exposure has persisted as a guiding line between privacy that is "reasonable" and privacy that is unreasonably expected, the Court has apparently done away with the "knowing" in knowing exposure. Indeed, one wonders whether, under the rule dispensed in later cases, Katz did not assume the risk that someone might bug a public phonebooth.[113] After all, doesn't one reserve the truly private matters to one's home, preferably with the shades drawn, or indeed to a bunker in the basement where there's no cell reception, and where all visitors are searched thoroughly for wires before entering?

The digital age has placed the third-party doctrine under even greater scrutiny. As Justice Gorsuch wrote in his dissent in *Carpenter*, the third-party doctrine makes us ponder, "What's left of the Fourth Amendment?"[114] In an age where we share almost everything with third parties, Justice White's "normative assessment of when a person should expect privacy" tells us that the answer is "never"—a "pretty unattractive societal prescription."[115]

Two main critiques can be levied against this assumption-of-risk framework. The first is that it is applied incorrectly: Many of the risks the Court presumed to have been taken were not really assumed in the first place. In *Smith*, for instance, the defendant himself did not know that the phone operator could keep a record of every number dialed on his telephone.[116] The Court found that the use of such records—through pen registers, at the time—was common knowledge.[117] The Court inferred such common knowledge from the fact that "[m]ost phone books tell subscribers, on a page entitled 'Consumer Information,' that the company 'can frequently help in identifying to the authorities the origin of unwelcome and troublesome calls.'"[118] If companies can identify such callers, naturally they keep a record of the numbers people dial, concluded Justice Blackmun, imposing such powers of deduction on every telephone owner in America.[119] But even if one assumes the risk that the phone company

126–37 (pointing out that, in practice, the doctrine does not create clarity but rather incoherence as it is applied differently in different cases).

113 *See supra* note 49 and accompanying text.

114 *Carpenter*, 138 S. Ct. at 2262 (Gorsuch, J., dissenting).

115 *Id.* at 2263.

116 Smith v. Maryland, 442 U.S. 735, 745 (1979).

117 *Id.* at 742 ("Although most people may be oblivious to a pen register's esoteric functions, they presumably have some awareness of one common use: to aid in the identification of persons making annoying or obscene calls.").

118 *Id.* at 742–43.

119 *Id.* at 748–49 (Marshall, J., dissenting) (questioning the assumption that "individuals somehow infer from the long-distance listings on their phone bills, and from the cryptic

does record dialed numbers, it does not follow that because one shared their information with one party, one is therefore voluntarily sharing it with the whole world. By this logic, Katz would have had no expectation of privacy in his conversation, because the person on the other end of the line could have been a gossip and told everyone about it.[120] As Justice Marshall noted in dissent, "[p]rivacy is not a discrete commodity, possessed absolutely or not at all."[121]

As currently applied, the third-party doctrine also often assumes information was voluntarily shared when individuals did not in fact have a choice. Can anyone truly choose not to open a bank account or own a telephone? In *California v. Greenwood*, the Court held that one has no expectation of privacy in the trash one leaves for collection on the sidewalk, "an area particularly suited for public inspection," despite the fact that almost all municipalities in the nation require that you dispose of your trash like so.[122] The Court assumed that individuals abdicated their right to privacy because "animals, children, scavengers [and] snoops" often rummage through trash left on sidewalks—and citizens must thus be aware of this risk when placing their trash bags outside.[123] It ignored, as Justice Brennan pointed out, the fact that just because someone *can* rummage through trash, that doesn't *entitle* them to do so.[124]

But a second critique of the third-party doctrine—more sweeping than noting errors in its application—is that it renders the Constitution hostage to haphazard techno-social developments. After all, the text of the Fourth Amendment is not conditional in its protection: It establishes and presupposes "[t]he right of the people to be secure in their persons, houses, papers and effects," regardless of whether someone is materially capable of violating this security.[125] In the face of this normative right, the assumption of risk standard amounts to Fourth Amendment victim-blaming. It distorts the Fourth Amendment as a rights provision and places it instead in the

assurances of 'help' in tracing obscene calls included in 'most' phone books, that pen registers are regularly used for recording local calls").

[120] *See Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting) ("People often *do* reasonably expect that information they entrust to third parties, especially information subject to confidentiality agreements, will be kept private.").

[121] *Smith*, 442 U.S. at 749.

[122] 486 U.S. 35, 35 (1988).

[123] *Id.*

[124] *See id.* at 54 (Brennan, J., dissenting); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2266 (2018) (Gorsuch, J., dissenting) ("'[I]t is common knowledge that plastic garbage bags left on or at the side of a public street are readily accessible to animals, children, scavengers, snoops, and other members of the public.' But the habits of raccoons don't prove much about the habits of the country." (citation omitted)).

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

Hobbesian realm of capability. In an age where technology significantly diminishes our privacy, and in which we need to use technology to meaningfully participate in society, the Fourth Amendment guarantees a right to be secure in one's private effects, and it is the Court's task to ensure this is so, rather than imposing a duty of secretiveness on individuals. Under the current interpretation, the Constitution protects only that which you can keep private. And, in the 2020s, unless you deal only in bitcoin transactions and use only burner phones, that is very little.

B. Exposure as Consent and Private Searches

In his dissent in *Carpenter*, Justice Gorsuch grappled with the notion of consent as supporting the third-party doctrine.[126] Indeed, the Fourth Amendment's consent exception has its own third-party framework—which is profoundly at odds with the rulings of *Smith* and *Miller*. The consent exception operates when the government argues that it did not intrude on constitutional interests because the subject of the search consented to being searched. When third parties are involved, this approach inquires whether they had the authority to consent to searches on behalf of the subject being searched—rather than assuming the government has broad authority to intrude wherever third parties have actually intruded.[127]

In *United States v. Matlock*, the Supreme Court cautioned that third-party consent is not automatic: The prosecution must show that "permission to search was obtained from a third party who possessed common authority over or other sufficient relationship to the premises or effects sought to be inspected."[128] Common authority, moreover, involves whether the third party enjoys "mutual use of the property," including "joint access or control for most purposes, so that it is reasonable to recognize that . . . [they have] the right to permit the inspection."[129] The Court engaged in a similar inquiry in *Frazier v. Cupp*, in which it found that Frazier had allowed his cousin constructive possession over his bag by leaving it in his cousin's house, and thus Frazier "must be taken to have assumed the risk that [his cousin] would allow someone else to look inside."[130] Likewise, in *Coolidge v. New Hampshire*, the Court found that it was necessary to assess

126 *See Carpenter*, 138 S. Ct. at 2263 (Gorsuch, J., dissenting).

127 United States v. Matlock, 415 U.S. 164, 170 (1974) ("The consent of one who possesses common authority over premises or effects is valid as against the absent, nonconsenting person with whom that authority is shared.").

128 *Id.* at 171.

129 *Id.* at 171 n.7.

130 Frazier v. Cupp, 394 U.S. 731, 740 (1969).

whether the defendant's wife, "in light of all the circumstances" had offered valid consent to a search on her husband's behalf.[131] Rulings since have inquired whether consent-based searches are based on consent that is valid—that is, whether consent was voluntary and freely given.[132]

Yet outside of the consent exception, third-party searches run into a parallel strand of the search doctrine that is itself irreconcilable with the third-party doctrine: private searches. The Supreme Court has maintained, since 1921, that third-party searches are outside the bounds of the Fourth Amendment, which only applies to government action.[133] Thus, where a third party conducts an unlawful search by trespassing on a subject's papers or office and then gives those documents to the government, the Fourth Amendment is not implicated.[134] According to the rule set forth in *Burdeau* and affirmed in *United States v. Jacobsen*, a private party may engage in an *unlawful* search or seizure and give the fruits of this search to the government without tainting the government's hands.[135] This reasoning assumes that the fruit-of-the-poisoned-tree inquiry begins and ends with the government, and that anything happening outside of the state's involvement is not relevant.[136]

These three subdoctrines—third-party consent searches, third-party private searches, and the third-party doctrine—reveal the fragmented nature of Fourth Amendment jurisprudence. Thus, if the government relies on consent, it needs to show that the third party had authority to consent on behalf of the searched subject.[137] But if it's unclear whether consent is at issue, or if the government does not rely on consent, the third-party doctrine standard focuses on expectations of privacy.[138] Yet, per the private search rule, no such standards are

---

131 Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

132 *See* Ohio v. Robinette, 519 U.S. 33, 40 (1996) ("The Fourth Amendment test for a valid consent to search is that the consent be voluntary, and voluntariness is a question of fact to be determined from all the circumstances." (citations and internal quotation marks omitted)); Bumper v. North Carolina, 391 U.S. 543, 548 (1968) ("When a prosecutor seeks to rely upon consent to justify the lawfulness of a search, he has the burden of proving that the consent was, in fact, freely and voluntarily given.").

133 Burdeau v. McDowell, 256 U.S. 465, 475 (1921).

134 *Id.* at 476.

135 466 U.S. 109, 113 (1984).

136 *Cf.* Wong Sun v. United States, 371 U.S. 471, 487–88 (1963) (excluding evidence obtained via coerced statements that were themselves excluded).

137 United States v. Matlock, 415 U.S. 164, 170 (1974).

138 *Compare id.* (finding that the constitutionality of the search depended on the scope of the third party's authority over the searched object), *and* United States v. Crisolis-Gonzalez, 742 F.3d 830, 835–36 (8th Cir. 2014) (same), *with* Walter v. United States, 447 U.S. 649, 656 (1980) (opinion of Stevens, J.) ("[A] wrongful search or seizure conducted by a private party does not violate the Fourth Amendment and . . . such private wrongdoing

necessary for third-party searches: In the 1980s, the Supreme Court maintained that, outside of situations where consent was alleged, the government need not inquire whether the third party's initial acquisition of information was lawful.[139]

It is difficult to reconcile these three doctrines. For one, the third-party consent exception and the private search doctrine have opposite views of the role of government in the transaction. While the consent exception requires an unbroken chain of consent from the subject searched to the third party and from the third party to the government, the private search doctrine treats this requirement as all or nothing: If the first chain link never comes to be (i.e., if the third party's original action is trespassory), then the remainder of the chain need not be legitimate either. For consent searches, on the other hand, there is no automatic assumption of risk, and courts will assess, even if only cursorily, the nature of the relationship between the subject of the search and the third party to determine whether the government's subsequent actions were legitimate or were the fruit of invalid consent to search.[140]

A second issue is one of incentives: Why should a private individual be more protected from government intrusion after they have *consented* to a third party's search than when this search was in fact unlawful? Such a rule hardly encourages third-party conduct to be within the bounds of legality. Indeed, it carves out a massive loophole on the already tattered cloak of Fourth Amendment protection, because where the government could not search without violating the Constitution, it can safely rely on third-party actors to search on its behalf, outsourcing constitutional infringement with impunity to corporations with vastly greater search capabilities.[141]

These disparate standards run into greater trouble now that modern third-party scenarios traverse these artificial legal distinctions. One example is a circuit split involving Google searches of files on its email provider, Gmail. Google employs an automatic detection

---

does not deprive the government of the right to use evidence that it has acquired lawfully.").

[139] *Walter*, 447 U.S. at 656; United States v. Jacobsen, 466 U.S. 109 (1984).

[140] *See supra* note 138 and accompanying text; *see also* Andrew MacKie-Mason, *The Private Search Doctrine After* Jones, 126 YALE L.J.F. 326 (2017) (discussing the applicability of *Jacobsen* to reasonable expectation of privacy cases).

[141] *See* Julia Angwin, Jeff Larson, Charlie Savage, James Risen, Henrik Moltke & Laura Poitras, *NSA Spying Relies on AT&T's 'Extreme Willingness to Help*,' PROPUBLICA (Aug. 15, 2015), https://www.propublica.org/article/nsa-spying-relies-on-atts-extreme-willingness-to-help [https://perma.cc/ZGK9-WW9Q] (reporting that government agencies like the NSA have relied on corporations' "direct access" to private data to engage in sweeping surveillance operations).

software known as "hash value matching" to flag when users upload what the software recognizes as child pornography.[142] Once this flag is raised, Google then sends a report to a federal agency, which traces the user's IP address.[143] The Sixth Circuit found that this process triggered no Fourth Amendment violation, because private searches cannot trigger the search doctrine. Thus, as long as the government did not reach beyond Google's initial search, there was no constitutional infringement.[144] But in *United States v. Wilson*, on an identical set of facts, the Ninth Circuit disagreed, finding that "the government search exceeded the scope of the antecedent private search" because Google employees had never actually seen the images; their algorithm merely flagged them, and the government then saw the actual pictures raised by that flag.[145]

Relying on the Supreme Court's recent caveat in *Carpenter*, the Ninth Circuit cautioned against "uncritically extend[ing] existing precedents," and signaled that because such flags by Google are "automated," the Roberts Court's rationale for sweeping searches might apply to such cases.[146] While it recognized that it was bound to apply the private search doctrine, the panel indicated that *Carpenter* may have disturbed *Jacobsen*, because the private search rule "rests directly on the same precepts" which "underlie the so-called third-party doctrine."[147] *Wilson* reflects a growing unease among lower courts where the private search rationale of the third-party doctrine is concerned, especially in light of *Carpenter*.[148]

The overlap of the consent, private-search, and third-party frameworks evinces their inconsistencies. But as Part III will describe, reconciling them is easier than it may appear. As *Carpenter* signals the intent to curtail the expanse of the third-party doctrine, the solution to the disagreement between Chief Justice Roberts and Justice Gorsuch lies not in the forward-looking guessing game of morphing constitutional interpretation to technological advances, but rather in a simpler return to first principles: defining what "knowing exposure" is. The solution to the "crazy quilt"[149] of the Fourth Amendment lies not in additional patches of exceptions and sub-doctrines, but rather in the

---

142 United States v. Miller, 982 F.3d 412, 417 (6th Cir. 2020), *cert. denied*, 141 S. Ct. 2797 (2021).

143 *Id.*

144 *Miller* relied on the "settled rule" of the "private-search doctrine" established in *Jacobsen*. *Miller*, 982 F.3d at 417–18.

145 13 F.4th 961, 971–72 (9th Cir. 2021).

146 *Id.* at 979–80 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2222 (2018)).

147 *Id.* at 971 n.9.

148 *See generally* Tokson, *supra* note 30 (compiling an anthology of these cases).

149 Smith v. Maryland, 442 U.S. 735, 745 (1979).

underlying common thread that silently unites all of these lines of jurisprudence.

III
A Unified Approach: Returning to Knowing Exposure

Katz's greatest failing was one of definition, and subsequent doctrines have read it as demanding secrecy in exchange for privacy. The paradox of this version of the Fourth Amendment is that though it does not conjure an Invisibility Cloak, it demands that in order to preserve your privacy in an era of intense surveillance, you devise one for yourself and wear it at all times. The *Katz* doctrine's "crazy quilt," after all, is full of holes.[150] Even today, we struggle to distinguish Katz's decision to speak (to a third party, mind you) in a public phone booth to which the "public" might predictably have access, from Wilson's decision to share the contents of his emails with Google. Subsequent doctrines have sought to answer this question obliquely, each with its own distinct line of cases. Neither sub-doctrine explains what knowing exposure is. Instead, the Court has continued to sew additional patches into its jurisprudential quilt, rather than returning to first principles.

It is the definition of this first principle that this Part seeks to provide. Post-*Carpenter* applications of the third-party doctrine should be distinguished based on whether the search's subject knowingly exposed themselves to the third-party agent. Knowing exposure, in turn, should be defined looking to whether it was (1) knowing, (2) voluntary, and (3) reasonable, applying a sliding scale, totality-of-the-circumstances approach congruent with the justifiable caution in Fourth Amendment doctrine. This Part defines, defends, and applies these elements to particular cases.

A. Knowing

In *Carpenter*, Chief Justice Roberts laid out the key problem: Some information "is not truly 'shared' as one normally understands the term."[151] CSLI, for instance, is logged by phone providers "without any affirmative act on the part of the user."[152] As a result,

---

[150] For a summary of similar criticism of the modern search doctrine, see Colb, *supra* note 23, at 189 (noting that the third-party doctrine both fails to "give adequate protection to privacy" and is incoherent, as "the very tests that the Court announces and applies in some contexts are contradicted and undermined in others").

[151] Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

[152] *Id.*

such activity is beyond the scope of the third-party doctrine.[153] Chief Justice Roberts's point suggests that to be knowingly exposed, the individual must have known—perhaps either actually or constructively—that the third party was collecting their information. The inquiry further involves a second requirement: The exposed individual must have had notice that the third party would then share this information with others.

The Supreme Court has already addressed the first prong of this inquiry—knowledge of third-party exposure—in multiple decisions, albeit unevenly. In third-party doctrine cases, knowledge has been an essential element of the inquiry, even if it is easily overcome. In *Smith*, for instance, the Court turned to constructive notice to find that telephone purchasers could have reasonably known about the existence of pen registers.[154] Likewise, *Miller* relied on the fact that individuals actually knew they were turning information over to banks when opening accounts.[155] In *Katz*, the petitioner's lack of knowledge that the phone booth was bugged was an essential element of his Fourth Amendment protection.[156] Of course, knowledge can be defined subjectively, objectively, and constructively, and in other surveillance cases, the Court transformed the concept of constructive or "common knowledge" into exposure due to ease of access by others, rather than the exposed person's awareness.[157] Any definition of knowledge can therefore turn into a slippery slope by a court who wants to construe knowledge out of nothing. For this reason, we must define knowledge based on what is *actually* known to the subject of a search.

Although the third-party doctrine does not address the second prong of this inquiry—the individual's knowledge about the scope of that exposure, particularly whether the third party will disclose the exposed information to others—the consent exception and the private search frameworks do.[158] *Matlock*, for instance, relied on the concept of "common authority" to delineate the boundary of third-party con-

---

153 *Id.*

154 Smith v. Maryland, 442 U.S. 735, 743 (1979) ("Telephone users, in sum, typically know that they must convey numerical information to the phone company.").

155 United States v. Miller, 425 U.S. 435, 442 (1976) (noting that bank checks were "not confidential communications but negotiable instruments to be used in commercial transactions," and that bank statements contained information "exposed to [bank] employees in the ordinary course of business").

156 The discussion in *Katz* centered on a "concealed electronic device," Katz v. United States, 389 U.S. 347, 355 (1967), which the Court said justified one's expectation that "the words he utters into the mouthpiece will not be broadcast to the world," *id.* at 352.

157 *See supra* Section II.A.

158 Landmark third-party doctrine *dissents*, however, do discuss scope. *See supra* Section II.A.

sent.[159] The private search doctrine similarly looks to whether the government search expanded beyond the scope of the private search.[160] The Court should unify these strands, extending these frameworks to the third-party doctrine and eliminating its broad categorical rule that once you disclose information to a third party, you "forfeit any reasonable expectation of privacy" in it.[161] Thus, the knowing exposure standard should entail two steps: First, courts should ascertain the legal validity of the original interaction involving information disclosure; and second, they should then look to whether the scope of that original exposure encompasses disclosures by the third party to others.

There are three reasons why importing this standard of knowledge as related to consent would make sense for the third-party doctrine. First, most modern third-party doctrine cases could easily be described as consent-based searches: The only reason most companies have access to your data is that, at least constructively, you have consented to their access.[162] Increasingly, surveillance occurs through adhesion contracts, rather than through peeping toms peering through roofs or holes in fences. Second, such an approach would avoid the loophole in private searches, through which the government outsources investigation to private actors and avoids constitutional scrutiny. By requiring the same standard to apply across search doctrine cases, this framework would overturn *United States v. Jacobsen*. Instead, it demands that knowledge be maintained throughout the transaction chain, not only between the subject of the search and the private actor, but also between the third party and the government.

Third, and most important, a knowledge-as-consent approach would center our understanding of the Fourth Amendment as a right, rather than demarcated by haphazard evolutions in technology. Moreover, as Justice Gorsuch observes, knowledge has a common law analogue: notice. Not only do we apply knowledge daily in other areas of the law, but the concept pre-dates the Fourth Amendment's text.[163]

---

159 *See generally* United States v. Matlock, 415 U.S. 164 (1974).

160 *See generally supra* notes 142–45 and accompanying text.

161 Carpenter v. United States, 138 S. Ct. 2206, 2262 (2018) (Gorsuch, J., dissenting).

162 *See* H. MARSHALL JARRETT, MICHAEL W. BAILIE, ED HAGEN & NATHAN JUDISH, OFF. OF LEGAL EDUC., EXEC. OFF. FOR U.S. ATT'YS, MANUAL: SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS 25 (3d ed. 2009) ("Significantly for Fourth Amendment purposes, commercial service providers typically have terms of service that confirm their authority to access information stored on their systems, and such terms of service may establish a service provider's common authority over their users' accounts.").

163 For an overview of the role of knowledge in the search doctrine, see generally Tokson, *supra* note 30.

This approach is not revolutionary in the law. Imposing knowledge standards on the Fourth Amendment would establish a long-overdue normative standard for a doctrine hitherto shaped by positive developments.[164]

B. Voluntary

Modern third parties often give individuals notice that their data is being tracked and shared with others, as is sometimes demanded by some international statutory and regulatory regimes.[165] But constructive notice can distort the concept of knowledge: The Court has extrapolated knowing exposure from the devised "common knowledge" that trash bags are accessible by snoops once left out on the street, or that people in planes can see into backyards, or that phone owners know about pen registers.[166] Solely applying a constructive notice standard would also render individuals' privacy prey to adhesion contracts.[167]

Such a standard must then be qualified: As *Carpenter* indicates, information is not "truly shared" unless one "*voluntarily* assume[s] the risk" of turning over one's private data.[168] Voluntariness is one step beyond knowledge, because while you may know for a fact that you are giving your bank your private information, and you may even be informed that the bank shares records with law enforcement, you live in a society where you have little choice but to open a bank account. Would the alternative be to stash cash under your mattress, or to own everything in bitcoin? Instead, you are not voluntarily

---

164 *Id.* at 194–203 (proposing a direct normative balancing approach to fully clarify the role of knowledge in search doctrine cases).

165 *See* Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES, https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us [https://perma.cc/H82M-H2HG] (describing Europe's comprehensive privacy law, the General Data Protection Regulation, and contrasting it with the scantier American protections). Moreover, the Federal Trade Commission has the power to investigate a corporation that violates its own privacy policy with regard to its users. *Id.*; *see also* Erin Mershon, *FTC Cracks Down on Snapchat*, POLITICO (May 9, 2014, 9:00 AM), https://www.politico.com/story/2014/05/snapchat-ftc-privacy-crackdown-106495 [https://perma.cc/W9C2-TA68] ("Snapchat deceived consumers by telling them that messages would 'disappear forever' when in fact they can be captured by recipients and other apps, according to the Federal Trade Commission, which announced a settlement with the company.").

166 *See generally supra* Part I.

167 See generally Wayne A. Logan & Jake Linfold, *Contracting for Fourth Amendment Privacy Online*, 104 MINN. L. REV. 101 (2019) for a discussion of the challenges adhesion contracts pose for privacy, and the ways lower courts have turned to the validity of such contracts as an ersatz replacement for Fourth Amendment protections.

168 Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (emphasis added) (internal quotation marks omitted).

assuming the risk of exposure, *Carpenter* unpacks, when you are relying on a service that is "indispensable to participation in modern society."[169] The Court has held that digital effects fit this definition.[170] But by extension so do owning a telephone, opening a bank account, and disposing of garbage.[171]

Carpenter's indispensability standard as a proxy for voluntariness fits the knowing exposure inquiry: Where data collection is automatic, it is not really voluntary. The Court may wish to inquire whether reasonable alternatives exist; for example, one may be able to switch to a messaging app that does not track or read message contents, so that subscription to a service like Facebook messenger, which reports user data to other parties, can be deemed voluntary.[172] On the other hand, if all email providers read message contents, then there has been no voluntary exposure—most people have email because they must, not because they enjoy receiving late-night work notifications.

C. Reasonable

But a final inquiry is required, based on the Court's signaling in *Carpenter*, as well as the concurring opinions in *Jones* and a few prescient dissents here and there.[173] A Court determining whether a Fourth Amendment violation has occurred must further ask whether the exposure, even if knowing and voluntary, was objectively reasonable from a societal perspective. As Justice Harlan argued in dissent in *United States v. White*, the Fourth Amendment is not about particularized conflicts in which positive-based concepts can easily apply. Rather than looking to individual risks, the task of the law is "to form and project" risks that we as a society undertake collectively.[174] The function of judges is not to "merely recite the expectations and risks without examining the desirability of saddling them upon society."[175] As technology has leaped forward with greater force, and as we have, perhaps unreasonably, exposed ourselves to third-party corporations,

169 *Id.* (citation omitted).

170 Riley v. California, 573 U.S. 373, 385–86 (2014).

171 *Carpenter*, 138 S. Ct. at 2234 (Kennedy, J., dissenting) (questioning the majority's distinction between *Carpenter* CSLI records and the bank records and phone records in *Miller* and *Smith*); *id.* at 2266 (Gorsuch, J., dissenting) (criticizing the result of California v. Greenwood, 486 U.S. 35 (1988)).

172 *See* Kate O'Flaherty, *Is It Time to Leave WhatsApp – And Is Signal the Answer?*, THE GUARDIAN (Jan 24, 2021, 2:00 AM), https://www.theguardian.com/technology/2021/jan/24/is-it-time-to-leave-whatsapp-and-is-signal-the-answer [https://perma.cc/E56N-ERGJ] (reporting that users seeking more privacy are leaving some apps for encrypted alternatives).

173 See generally *supra* Section I.B and Section II.A for these prescient dissents.

174 United States v. White, 401 U.S. 745, 786 (1971) (Harlan, J., dissenting).

175 *Id.*

Justice Harlan's words serve as a stark reminder that the Court's job is to stay true to the Fourth Amendment—even in a world that increasingly defies its premise.[176]

In order to properly exercise this function, the Court must then also look to whether the disclosure, especially in the aggregate level, is one that reveals such intimate details on such a sweeping scale that it is inconsistent with the purpose of the Fourth Amendment.[177] This inquiry looks to the reasonableness of the actual disclosure, rather than merely the reasonableness of the expectation of privacy. For example, even if some young social media users willingly and knowingly share their facial information with TikTok or Instagram, may these companies turn this information over to the government to implement large-scale facial recognition programs with the goal of crime prevention? Would such a turnover of information be consistent with the meaning of the Fourth Amendment? The reasonable inquiry would thus give courts the opportunity to pause on intensive information sharing and allow the Fourth Amendment to perform its protective function. The Court may ask whether the meaning of the Constitutional provision is consistent with this degree of warrantless governmental access to individual data. Such an objective inquiry focuses not necessarily on the case at hand, but on the government's position before its citizens, guilty and innocent alike.

Some have argued that this "reasonableness" inquiry lies with the legislature rather than the Court, and that sweeping constitutional law may not be the best avenue to address it.[178] The democratically elected bodies, this argument goes, ought to determine what "reasonableness" is within the meaning of the Fourth Amendment, especially because our society's conception of privacy evolves with the times. While this is indeed true, the question of what the Fourth Amendment means remains the purview of constitutional law. Just as the Court has not shied away from delineating the boundaries of First and Second

---

[176] *See also* Arnold H. Loewy, *The Fourth Amendment as a Device for Protecting the Innocent*, 81 MICH. L. REV. 1229, 1252–53 (1983) (distinguishing that the Court's logic makes sense from the perspective of guilty defendants, but not as "[a]s applied to the innocent"); William Baude & James Y. Stern, *The Positive Law Model of the Fourth Amendment*, 129 HARV. L. REV. 1821, 1823 (2016) (arguing generally that "Fourth Amendment protection should be anchored in background positive law").

[177] The "Mosaic Theory" as applied by Justice Sotomayor in her concurrence in *Jones* would fall under this category. *See* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (stressing the importance of looking to aggregation as a factor); Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 314 (2012) (describing this approach as one that "aggregat[es] conduct rather than looking to discrete steps" to assess whether there has been a privacy intrusion).

[178] *See* Kerr, *New Technologies*, *supra* note 15 (arguing that legislatures are better equipped to adapt Fourth Amendment protections to new technologies).

Amendment protections, which are also affected by technological changes, neither should it hesitate to do so for Fourth Amendment protections. The question of what constitutes constitutional Fourth Amendment reasonableness may be answered with a variety of tools, including originalist intent, modern definitions of reasonable exposure rooted in positive law, and policy considerations in light of the Amendment's overarching purpose. The reasonableness inquiry need not be a catch-all provision, but it can serve as a saving grace against sweeping or "dragnet" third-party searches.[179] A sliding scale approach would allow the Court to at least consider it as a factor when assessing the constitutionality of such issues, inquiring whether the exposure is so great as to be unreasonable, especially in light of lack of voluntariness or knowledge.

D. Knowing Exposure Applied

The search doctrine has long been splintered into different lines of decisions, based on particular fact patterns. The traditional third-party cases, like *Smith* and *Miller*, have focused on constructive knowledge to delineate the boundary of constitutional protection.[180] The consent-based search decisions, such as *Matlock*, focus on consent as the source of the government's valid intrusion.[181] Finally, the private search cases, such as *Jacobsen* and *Walter*, protect the government from any constitutional liability if its searches are conducted through a third party.[182] While these different strands of doctrine are legally confusing, factually, all of these cases are similar. They all involve a private third party accessing information and then turning it over to the government. And, as we see in recent cases, the overlap between these doctrines has become increasingly difficult to ignore: *Carpenter* was similar to *Smith* and *Miller*, but Chief Justice Roberts inquired into whether the subject of the search had given valid, voluntary consent to the third party; and the 2021 circuit split involving Google's automatic email search for child pornography also gave rise to third-party, private search, and consent questions.[183]

A unified knowing exposure standard would recognize that these fact patterns all involve the same problem and should be addressed the same way. It would also refine the reasonable expectation of privacy test, because, in treating external access to information as a proxy for knowing exposure, it obliterates the distinction of knowing

---

179 Carpenter v. United States, 138 S. Ct. 2206, 2231 (2018).

180 *See supra* Section II.A.

181 *See supra* notes 127–29 and accompanying text.

182 *See supra* notes 133–39 and accompanying text.

183 See *infra* Section III.D.3 for a discussion of this circuit split.

exposure altogether. This subsection applies the knowing exposure test to these four key doctrinal lines—traditional third-party doctrine cases, content searches, private searches, and reasonable expectation of privacy cases—to demonstrate why a unified standard that returns to basic first principles, outlined in *Katz*, emerges as the common thread in the patchwork of different Fourth Amendment decisions.

1. Carpenter*,* Miller*, and* Smith*: Traditional Third-Party Doctrine*

The three prongs of knowing exposure are salient in *Miller* and *Smith*. In both cases, the Court found that no expectations of privacy existed in information turned over to third parties for three reasons: First, the information was knowingly disclosed to third parties; second, the information was voluntarily disclosed; and thirdly, such an expectation of privacy was not one that society was prepared to consider reasonable.[184] In applying the same test to CSLI, *Carpenter* veered away from the assumption of risk theory without stating so outright. Instead, the information here was so revealing, and the surveillance so inescapable, that one could not be said to be assuming the risk of knowing exposure.[185] In dissent, Justice Gorsuch chastised the Court for refusing to overturn *Miller* and *Smith* while applying an indistinguishable standard, with vague factors to determine whether the information was sweeping.[186]

But instead of trying to reconcile *Carpenter* with the traditional third-party doctrine based on assumption of risk, we may best understand *Carpenter* as a reimagining—or re-analyzing—of knowing exposure. One way of thinking about the ruling is, from Justice Gorsuch's perspective, that it failed the scope of knowledge prong: Maybe Carpenter had shared information on his location to his phone provider, but "[c]onsenting to give a third party access to private papers that remain my property is not the same thing as consenting to a *search of those papers by the government.*"[187] Although Chief Justice Roberts did not address the scope of knowledge question, the majority opinion made it clear that, regardless of the knowledge prong, the facts here failed the other two: The disclosure was neither voluntary, by virtue of being automatic and inescapable, nor reasonable from a societal standpoint, given its sweeping nature.[188] The four factors from *Carpenter*—(1) how revealing the information was;

[184] *See* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (describing these decisions).

[185] *Id.* at 2216–17.

[186] *Id.* at 2267 (Gorsuch, J., dissenting).

[187] *Id.* at 2263.

[188] *Id.* at 2220.

(2) the degree of exposure; (3) the aggregate effect of such surveillance on society; and (4) the inescapability of surveillance to invalidate the assumption of risk reasoning—can thus be reconstructed into the two other prongs of knowing exposure.[189] The first three fall within the reasonableness inquiry and address our society's collective interest on the "aggregate effect" of such surveillance; and the fourth one inquires whether the disclosure was truly voluntary.

What about *Miller* and *Smith*, left on life support? The Court can overrule both, noting that, at least today, both banking and dial phones are as "indispensable" and "inescapable" as cellphones.[190] Alternatively, in "stealth overruling" fashion,[191] the Court can distinguish them on the reasonableness and voluntariness prong, without addressing the scope of knowledge inquiry. In all scenarios, the scope of knowledge problem is virtually the same: To what extent is your disclosure of information to your bank, your phone company, or your cellphone service provider, consent to government intrusion? But if the Court were to adopt a sliding-scale, totality-of-the-circumstances approach, it need not run the risk of "embarrassment" in admitting that *Smith* and *Miller* were wrongly decided (though that might be more honest).[192] Instead, the Court may opt to distinguish the cases, noting that the amount of information collected in *Carpenter* is simply too much and too damning for society, in a way that the pen register and the bank records are not. Or perhaps, phones were not so indispensable in the 1970s as they have become today, and thus their use was more voluntary then. Although these distinctions are no more convincing than Justice Roberts's, they illustrate that a sliding scale approach gives the Court the flexibility to reorder past decisions along a cohesive doctrinal line. And such flexibility would allow it to slowly build the search doctrine into a unified, cogent standard.

2. Consent Exception Searches

When it comes to the consent exception, courts treat consent as an express waiver of constitutional rights, and thus are required to assess whether such a waiver was knowing ("intelligent") and volun-

---

189 *See supra* note 90 and accompanying text.

190 Carpenter v. United States, 138 S. Ct. 2206, 2210, 2223 (2018); *see also supra* note 90 and accompanying text.

191 *See generally* Barry Friedman, *The Wages of Stealth Overruling (with Particular Attention to* Miranda v. Arizona*)*, 99 GEO. L.J. 1 (2010) (exploring the Supreme Court's "stealth overruling" of past decisions by simply distinguishing past cases instead of expressly overturning precedent).

192 *Id.* at 33–34 (identifying publicity as a cost to the Supreme Court and a reason not to explicitly overrule precedent).

tary.[193] In *Matlock*, for instance, the government obtained permission to search from a third party, and, while the Court approved the search as constitutional, it emphasized that such consent is not automatic. Instead, the Court relied on the common authority test, which looks to whether the third party does have in fact the authority to consent on another's behalf.[194] Notice the similarity between this approach and the Court's discussion in *Miller* of the fact that bank statements were property belonging to the bank as well as to Mr. Miller.[195] This concept of common authority can be used to delineate the scope of one's knowledge of exposure. At the same time, however, it is equally vague as the distinction between *Miller* and *Carpenter*: Is there a reason, after all, why the cell service provider did not "own" or have "common authority" over their users' location information? The Court may wish to distinguish the two cases based on the particular nature of CSLI, which involves an individual's particular location. However, no attempt has been made to protect location information in other scenarios, such as those involving license plate readers.[196]

Instead, reconciling the inquiry for consent in third-party consent searches with the inquiry for the third-party doctrine at large is an easier endeavor if we recognize that the fact patterns in *Carpenter* and *Matlock* are conceptually similar. In one sense, a provider like Google may argue that they are consenting to a government search on their users' behalf. From a knowing exposure perspective, then, it makes sense to assess the interaction between Google and its users according to a unified standard: Although users consent to information disclosure to *Google* as their email provider, such consent is not clearly delineated as a consent to *government* surveillance. Thus, as discussed in Section III.A, the scope of knowledge needs to be further clarified, and the Court has the precedent of *Matlock* as authority to establish it.

In addition to knowledge, the voluntariness inquiry is also part of consent search doctrine. In this line of cases, the Court has assessed whether a disclosure was indeed voluntary.[197] While the Court currently relies on a totality-of-the-circumstances approach to determine

---

[193] *See, e.g.*, Illinois v. Rodriguez, 497 U.S. 177, 183 (1990) ("We have been unyielding in our insistence that a defendant's waiver of his trial rights cannot be given effect unless it is 'knowing' and 'intelligent.'" (first quoting Colorado v. Spring, 479 U.S. 564, 574–75 (1987); and then quoting Johnson v. Zerbst, 304 U.S. 458 (1938))).

[194] See *supra* notes 128–32 and accompanying text for a description of the test.

[195] *See supra* note 108 and accompanying text.

[196] *See* United States v. Knotts, 460 U.S. 276, 281 (1983); Cardwell v. Lewis, 417 U.S. 583, 590 (1974).

[197] *See* Schneckloth v. Bustamonte, 412 U.S. 218, 248–49 (1973) (establishing a totality-of-the-circumstances approach to determine voluntariness).

voluntariness, the knowing exposure standard amounts to virtually the same rule. The goal of the voluntariness inquiry is to assess whether the subject of a search consented—either formally, by actual consent, or informally, through exposure—to the alleged constitutional intrusion. In *United States v. Drayton*, for instance, police conducted a search in Greyhound buses after the bus driver consented to a general search of the bus.[198] Although the government relied on the consent exception, one can imagine that if the bus company kept electronic records, the government could have also relied on the third-party doctrine to access those. In both scenarios, the voluntariness of the exposure is necessary, or petitioners will "theory shop" when filing Fourth Amendment suits.

The Court has also imported the reasonableness language from the Amendment's text into the consent analysis: In *Illinois v. Rodriguez*, Justice Scalia, writing for the majority, held that the police are allowed to rely on the consent exception if they "reasonabl[y] belie[ve]" there is common authority validating consent.[199] Adopting the "general rule" of reasonableness into the consent exception, the Court infused into its analysis normative values about what a society should or does consider reasonable, such as the need for officers acting in ignorance of fact to feel free to make mistakes, so long as those are reasonable mistakes.[200] The reasonableness prong thus also pervades the consent exception inquiry, and recognizing its existing function allows us to fashion the search doctrine into a more uniform line of cases.

3. *The Private Search Loophole:* Jacobsen *and the Gmail Circuit Split*

The private search doctrine does not survive knowing exposure analysis. The Supreme Court has not ruled on it since the Burger Era, and likely for good reason. The doctrine, a rebuff of the exclusionary rule, is difficult to justify when it comes to carving boundaries of Fourth Amendment protection.[201] For one thing, if your ultimate goal were to erode the Fourth Amendment, it would be difficult to resist the temptation of characterizing third-party doctrine cases as private

198 536 U.S. 194, 197–200 (2002).

199 Illinois v. Rodriguez, 497 U.S. 177, 183 (1990).

200 *Id.* at 186.

201 *See generally* John M. Burkoff, *Not So Private Searches and the Constitution*, 66 CORNELL L. REV. 627 (1981) (criticizing the doctrine as stated in *Burdeau v. McDowell* and *Walter v. United States* and arguing that it makes sense solely as an exception to the exclusionary rule, rather than as a full carve-out to constitutional protections over searches).

searches. After all, what distinguishes the cellphone provider in *Carpenter* from the mail provider in *Jacobsen*? In the Ninth Circuit, the private search loophole means that the government cannot currently rely on Google's hash value program for child pornography investigations, but if a criminal hacker organization were to access these emails and turn them over to the government, the government would have legitimate claim to such information.

The private search doctrine allows the government to access disclosures that are neither knowing, voluntary, nor reasonable. In *Jacobsen*, the subject of the search had no idea that his mail had been opened by the third-party mail carrier.[202] Even if the carrier had required consent to perform such searches of its clients, mail is as indispensable a service as they come, and use of mail carriers is hardly voluntary.[203] Yet, as the Ninth Circuit remarked in *Wilson*, the private search doctrine "rests directly on the same precepts" as the third-party doctrine.[204] In this sense, it's difficult to reconcile the private search exception with *Carpenter*, which requires that the government justify its intrusion as resulting from knowing exposure.

Finally, the loophole is unreasonable both in its allowance for violation of positive law by third parties and in its incentivization of the government to use private searchers to avoid constitutional liability. As Justice White noted, the private search exception means that "[i]f a private party breaks into a locked suitcase, a locked car, or even a locked house," they could obtain information for the government, and the latter could then "duplicate the prior search" with impunity.[205] In the modern era of contractor surveillance, such an exception threatens to swallow the entirety of the Fourth Amendment and is doubly irreconcilable with the other strands of the doctrine.[206] Logically, the private search doctrine is reconcilable with the knowing exposure standard as a case solely about the exclusionary rule, rather than the constitutional scope of Fourth Amendment protection.[207]

---

[202] *See* United States v. Jacobsen, 466 U.S. 109, 109 (1984) (describing how FedEx agents opened respondent's package, which had been damaged by a forklift, to assess contents for an insurance claim, presumably without first contacting respondent).

[203] *Cf. Ex parte* Jackson, 96 U.S. 727, 733 (1878) (holding that the content of letters and sealed packages deposited in the mail could be examined only upon the issuance of a warrant).

[204] United States v. Wilson, 13 F.4th 961, 971 n.9 (9th Cir. 2021).

[205] *Jacobsen*, 466 U.S. at 132 (White, J., concurring in judgment).

[206] *See* Angwin et al., *supra* note 141 (reporting that AT&T sifts through millions of emails and other data shared through its network and that because the NSA does not have "direct access" to telecoms' internet hubs, the private corporation will instead do the searching for the government without warrants or Fourth Amendment concerns).

[207] See generally Burkoff, *supra* note 201, for a similar assessment.

Such a distinction is unworkable, however, in a world where the exclusionary rule is the main remedy for Fourth Amendment violations.[208]

How would the knowing exposure standard resolve the Gmail circuit split?[209] When it comes to Google's hash value matching searches for child pornography, the knowing exposure framework would center on whether the original disclosure—from the user to Google—was knowing and voluntary. This would depend on whether Google presents its users with terms of service that not only inform them of the hash value matching system, but further give them notice that any flags through the software will send images to the government. Such a burden on Google would be minimal and would allow it to run its software program to protect its users from the evils of child pornography. Additionally, the government would have to show that using Google to retrieve such images is voluntary rather than indispensable. Here, child pornographers are hardly the ideal plaintiffs for Fourth Amendment protections in the digital age—a court would be hard-pressed to find that one "involuntarily" uploads child pornography images via email. But this case evinces that the contours of the voluntariness inquiry are still being designed, and that there is room to explore the ideal balancing of these competing factors. A court could refine these contours by asking whether the service is indispensable for the specific purpose, or by inquiring whether the specific purpose being serviced is itself indispensable.

The reasonableness inquiry would then assess the degree of exposure that the hash value matching software imposes on individuals, aiming to ascertain whether this exposure is itself socially reasonable. Relevant factors in the specific context of the Gmail hash value matching software would be whether the software flags only specific images; how likely it is to make a mistake and turn over other images to the government; whether the software reads every image to find flags, etc. By considering society's collective, normative values in Fourth Amendment rights, this reasonableness inquiry would encompass Justice Roberts's "sweeping" surveillance test and supplement it with Justices Harlan's and Brandeis's concerns for the role of the Supreme Court in safeguarding the central premise of the Fourth Amendment, which tends to be given up in piecemeal fashion by individual citizens over time.

In a scenario like *Wilson* and *Miller*, the knowing exposure standard has the particularly salient benefit of unifying different, irreconcilable doctrines which overlap in certain fact patterns. After

---

208 *Id.*

209 *See supra* notes 142–51 and accompanying text.

Carpenter, the standard for third-party searches is stricter than the analysis a court would rely on if it saw the facts as a classic private search. Similarly, a reliance on the consent exception would trigger a separate analysis with a different standard of protection. Yet all of these strands of the search doctrine emerge from the same constitutional provision, and as technology forces the overlap of these doctrines in fact, the Court must eventually acknowledge that they ought to be unified in law.

4. Reasonable Expectation of Privacy Reframed

Finally, the knowing exposure standard would have the added benefit of reconciling the third-party assumption of risk standard with the "access" based doctrine—the reasonable expectation of privacy test of *Ciraolo* and *Knotts*. While the Court currently defaults to the objective reasonableness prong of the Harlan test, which focuses on whether "society is prepared to recognize [an expectation] as reasonable,"[210] a global, unified knowing exposure test would more easily address fact patterns that transverse different strands of the doctrine.

Take, for instance, *Jones*, the GPS car search the Court ruled unconstitutional on property trespass grounds.[211] Although many blasted Justice Scalia for focusing on the arbitrary touching between a GPS device and the car, the court was split on how to protect Jones's privacy on alternative grounds. The reasonable expectation of privacy test had, after all, eliminated privacy expectations for cars traveling on public roads.[212] Yet what would the Court do if faced with a case in which the GPS tracking occurred entirely virtually, without trespass allegations? Under the private search approach, if the GPS provider simply turns the information over to the government, there has been no harm at all. Or perhaps the GPS purchase imposed contractual privacy terms upon the user, so that the user had fair notice that he was voluntarily turning over information that might be used by the government. Or, such a result might produce the kind of "sweeping" surveillance which concerned Chief Justice Roberts in *Carpenter*, and then trigger a different result. After all, while Chief Justice Roberts insisted that his opinion did not disturb existing precedent for other forms of surveillance, can we really distinguish driving, which in America is fairly indispensable and personal, from our movements recorded by our phones?

---

[210] Smith v. Maryland, 442 U.S. 735, 743 (1979) (quoting Katz v. United States, 389 U.S. 347, 361 (1967)) (internal quotation marks omitted).

[211] United States v. Jones, 565 U.S. 400 (2012).

[212] United States v. Knotts, 460 U.S. 276, 281 (1983).

A knowing exposure approach would encompass these different frameworks. The Court would assess whether Jones's original exposure to the GPS software was itself knowing and voluntary: Did Jones install the device himself? Did it come with the car, and was Jones aware of this when he purchased the vehicle or drove around in it? Did Jones understand what sharing his location with the GPS provider entailed? The answer to these is most likely *yes*, unless, as in the actual *Jones* case, the device was installed without the driver's knowledge.[213] Then, we ask whether Jones knowingly and voluntarily shared the information *with the government*. Did the GPS provider give him valid notice that his location might be shared with others? How constructively would a court have to stretch the letter of this notice? Is the contract clear? On the voluntariness prong, the Court would inquire whether Jones had any choice in the matter: Do all cars come with GPS devices these days? Can you yank yours out of the dashboard if you don't want to be tracked?

Notice that, once again, the facts are likely to also pass the second prong, but the burden falls to the third party to clearly notify its clients of the degree to which it uses their shared data. Perhaps this burden is not sufficient; perhaps we have, as a society, determined that we don't care about our privacy rights as much as we enjoy the conveniences of technology. If this is the case, the Court may avail itself of the third prong, *reasonableness*, as a final safeguard of Fourth Amendment protections.

Reasonableness is, after all, the Fourth Amendment's textual protection against government intrusion. It allows courts to weigh the degree to which the internet's ocean of data can help law enforcement keep an increasingly globalized world safe, and this Note does not dispute this fact. But by allocating the determination of *reasonable* searches and seizures to the Constitution, the text of the Fourth Amendment immunizes it from extrinsic erosion. Precisely because surveillance requires forethought and strategy, the role of a judge is not only reasonable but rather fitting before law enforcement sets out to request third parties to turn over this plethora of information.

The Bill of Rights enumerates overarching principles to which we as a society contracted centuries ago. Just as the First Amendment is not cast away if we start censuring each other in local communities, or the Second is not thrown out if we stop buying guns, so too is the meaning of the Fourth independent of practices that threaten its protections. The Court's task is to guard it against these forces, not to yield to them.

---

[213] *Jones*, 565 U.S. at 413 (2012) (Sotomayor, J., concurring).

Conclusion

Carpenter left the search doctrine unraveled, struggling to reconcile different strands of the search doctrine with the risks that evolving technology poses for privacy. Yet, while the Orwellian threat of big tech creeps in, the Court finds itself entwined in its own logical loopholes across different Fourth Amendment sub-doctrines, trying to clarify the reasonable expectation test from *Katz* in light of its developments in third-party searches, consent-based searches and private searches. This Note assesses this "crazy quilt" of the Fourth Amendment and finds a common thread across its different patches: the concept of knowing exposure.

As the Supreme Court seeks to modernize the Fourth Amendment to the modern age, it should remember that the universalization of data-collection renders the facts of one case generalizable not only to the defendant at hand, but to all members of our tech-dependent society. And while this may be a Faustian bargain of our own doing, Fourth Amendment jurisprudence ought not to center around assumption of risk of the facts at hand, or the apparent guilt of one defendant, but rather on principles and values that extend to all of society. In this sense, perhaps the silver lining in the digital era might be that it will finally force us to confront the fact that constitutional protections exist to protect the innocent as well as the guilty. Because, when it comes to losing our privacy, we are all losing it together.