VIRGINIA LAW REVIEW ONLINE

VOLUME 111 AUGUST 2025 188–214

ESSAY

FOURTH AMENDMENT TRESPASS AND INTERNET SEARCH HISTORY

*Alec J.H. Block & Joseph W. Paul**

Browsing the internet is an everyday activity for many Americans. Law enforcement has capitalized on this reality by employing a novel investigative technique: reverse keyword search warrants. Keyword warrants allow investigators to obtain detailed information from search engine companies about any internet user who entered a specific phrase into the search engine. In recent years, the constitutionality of these warrants has sparked growing debate. Underlying this debate rests a critical threshold question: Does the Fourth Amendment require the government to obtain a valid warrant before accessing a person's internet search data? Thus far, three courts have addressed the question, all reaching different conclusions.

One reason for the lack of consensus is that these courts have relied exclusively on the "reasonable expectation of privacy" test to determine whether a warrant is required to access search data. This Essay explains why assessing search data under the privacy framework leads to muddled analysis and contradictory conclusions, contributing to constitutional uncertainty. We urge courts to look instead to the

* J.D. Candidates, University of Virginia School of Law, expected 2026. We are indebted to Professors Anne Coughlin, Thomas Frampton, Josh Bowers, Daniel Epps, and Richard Re for their thoughtful feedback. We also thank Brian Curtis, Ella Missan, and the entire *Virginia Law Review* team for their help in bringing our Essay to publication.

traditional trespass test set out in United States v. Jones *to determine whether the Fourth Amendment protects search data. By analyzing the issue through the lens of trespass, this Essay reaches a clear answer: accessing search data is a Fourth Amendment search. In doing so, this Essay adds urgency to the keyword warrant debate, advances Fourth Amendment doctrine in a rapidly evolving technological landscape, and helps realize the full protections of that constitutional guarantee.*

INTRODUCTION

On July 19, 2016, someone broke into a Pennsylvania home and assaulted the woman living there.[1] After spending two months exhausting their physical leads, law enforcement was still without a suspect.[2] So, investigators turned to Google.[3] Specifically, they obtained a warrant directing Google to disclose detailed information associated with any user who searched the victim's name or home address in the week preceding the attack.[4] This novel investigative technique, known as a "keyword warrant,"[5] led investigators to John Edward Kurtz, who was later charged and convicted.[6] On appeal, Kurtz challenged the warrant as unconstitutional, arguing that its omission of a named suspect violated the Fourth Amendment's probable cause and particularity requirements.[7] The constitutional sufficiency of the warrant was ultimately irrelevant to the case, however, because the court held that government access to Kurtz's

[1] See Commonwealth v. Kurtz, 294 A.3d 509, 516–17 (Pa. Super. Ct. 2023), *appeal docketed*, 306 A.3d 1287 (Pa. 2023).

[2] See Appellee's Brief at 7–8, 12, *Kurtz*, 294 A.3d 509 (No. 811 MDA 2021).

[3] *Kurtz*, 294 A.3d at 517.

[4] Id.

[5] Both throughout the literature and within this Essay, "keyword warrants" are referred to interchangeably as "keyword search warrants" or "reverse keyword search warrants." For additional discussion regarding the mechanics of keyword warrants, see Helen Winters, Note, An (Un)reasonable Expectation of Privacy? Analysis of the Fourth Amendment When Applied to Keyword Search Warrants, 107 Minn. L. Rev. 1369, 1387–89 (2023).

[6] *Kurtz*, 294 A.3d at 516–18.

[7] Appellant's Brief at 12, 19, *Kurtz*, 294 A.3d 509 (No. 811 MDA 2021). The constitutionality of keyword warrants has received significant attention. Some commentators have argued that keyword warrants are unconstitutional general warrants. See Chelsa Camille Edano, Comment, Beware What You Google: Fourth Amendment Constitutionality of Keyword Warrants, 97 Wash. L. Rev. 977, 1000–02 (2022); Brian L. Owsley, Searching a Person's Thoughts: Keyword Search Warrants and Fourth Amendment Concerns, 28 Stan. Tech. L. Rev. 66, 102–03 (2025). Others have articulated theories supporting the warrants' constitutionality. See Mary D. Fan, Big Data Searches and the Future of Criminal Procedure, 102 Tex. L. Rev. 877, 925–27 (2024).

search data was not a search at all.[8] Thus, no valid warrant was required to obtain his search data.[9]

Commonwealth v. Kurtz raises a pressing question: Can the police access your internet search history without a warrant? Because it is not clear that a keyword warrant can ever be validly issued, the constitutionality of keyword searches may depend on the threshold question of whether it is a Fourth Amendment "search" that requires a warrant.[10] As of this writing, however, no consensus answer has emerged: three state courts have addressed the question, and they have all reached different conclusions.[11] One reason for this uncertainty is that courts have relied on the familiar "reasonable expectation of privacy" framework to answer the threshold search question.[12]

This Essay seeks to change that. Part I explains why applying the reasonable expectations test to search data produces contradictory results. Part II urges courts to look instead to the traditional trespass test endorsed in *United States v. Jones* to determine whether the Fourth Amendment protects search data. Though the Supreme Court has never applied the trespass test to intangible property, we explain why adopting this approach in the context of search data is consistent with Fourth Amendment jurisprudence and produces a clear answer: accessing search data is a search. Finally, Part III addresses the limitations of our trespass analysis and explores its impact on existing case law.

I. SEARCH DATA AND EXPECTATIONS OF PRIVACY

In 1967, *Katz v. United States* introduced a new constitutional test, which is now recognized as the "touchstone" of modern Fourth

[8] *Kurtz*, 294 A.3d at 522.

[9] The Fourth Amendment's protections are not triggered unless a search or seizure occurs. County of Sacramento v. Lewis, 523 U.S. 833, 843 (1998).

[10] See supra note 7.

[11] Compare *Kurtz*, 294 A.3d at 522 (finding that no Fourth Amendment search occurred when the government used a keyword warrant), with People v. Seymour, 536 P.3d 1260, 1272 (Colo. 2023) (finding that a keyword warrant constitutes a search, but only under Colorado's Constitution and not the Fourth Amendment), and Commonwealth v. Clements, 113 Va. Cir. 576, 591 (2024) (finding that the government engaged in a Fourth Amendment search when it employed a keyword warrant). No federal court has published an opinion addressing the question.

[12] See *Kurtz*, 294 A.3d at 521–23 (engaging exclusively with the *Katz* reasonable expectation of privacy framework when considering whether a keyword warrant is a search); *Seymour*, 536 P.3d at 1270–72 (same); *Clements*, 113 Va. Cir. at 590–91 (same).

Amendment search analysis.[13] Under *Katz*, a search occurs when the government violates an individual's "reasonable expectation of privacy."[14] Although courts often struggle to determine what expectations of privacy are "reasonable,"[15] for decades one rule simplified the task in certain contexts. Under the third-party doctrine, a person has no reasonable expectation of privacy in information they voluntarily disclose to third parties.[16] While the third-party doctrine long represented a "bright-line" rule,[17] the landmark case *Carpenter v. United States* rearticulated the doctrine in response to new technology.[18] After *Carpenter*, individuals may retain a reasonable expectation of privacy in digital information they share with others, at least in certain circumstances.[19]

The issue in *Carpenter* was whether a search occurred when law enforcement accessed seven days of cell site location information ("CSLI") held by the defendant's cellular provider.[20] Despite its third-party exposure, the Court held that the CSLI was protected by the Fourth Amendment because it could "provide[] an intimate window into a person's life" and was "not truly 'shared' as one normally understands the term."[21] Given the Court's reasoning, scholars generally agree that *Carpenter* protects digital information that is (1) intimate and (2) involuntarily exposed to a third party.[22] Like CSLI, search data is exposed

[13] Oliver v. United States, 466 U.S. 170, 177 (1984) (citing Katz v. United States, 389 U.S. 347, 360 (1967) (Harlan, J., concurring)).

[14] See 389 U.S. at 360–62 (Harlan, J., concurring).

[15] See Carpenter v. United States, 138 S. Ct. 2206, 2213–14 (2018) ("[N]o single rubric definitively resolves which expectations of privacy are entitled to protection . . . ."); Orin Kerr, The Digital Fourth Amendment: Privacy and Policing in Our Online World 16 (2025) [hereinafter Kerr, Digital Fourth Amendment] (describing the reasonable expectation of privacy test as "a source of endless confusion").

[16] Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); see United States v. Miller, 425 U.S. 435, 443 (1976).

[17] United States v. Caira, 833 F.3d 803, 806 (7th Cir. 2016).

[18] 138 S. Ct. at 2216–20.

[19] Id.

[20] Id. at 2211–13, 2217 n.3.

[21] Id. at 2217, 2220.

[22] See, e.g., Matthew Tokson, The *Carpenter* Test as a Transformation of Fourth Amendment Law, 2023 U. Ill. L. Rev. 507, 518 (2023) (identifying a *Carpenter* test that looks to "(1) the revealing nature of the data collected; (2) the amount of data collected; and (3) whether the suspect voluntarily disclosed their information to others"); Kerr, Digital Fourth Amendment, supra note 15, at 153–54 ("First, the records must be of a new type made

to a third party (the search engine) when the user enters search queries. It is therefore unsurprising that every court addressing the Fourth Amendment implications of search data has looked to *Carpenter* for guidance.[23] Unfortunately, these courts have applied the opinion in radically different ways, reaching contradictory results.

Start with *Carpenter*'s intimacy prong. Courts are split on an important threshold issue: Is the relevant question whether *search data generally* is an intimate type of information or instead whether *the specific request at issue* may reveal intimate details about the user? *Commonwealth v. Kurtz* applied *Carpenter* by evaluating the intimacy of the particular search terms that law enforcement had requested in the instant case.[24] Reading *Carpenter* this way, the court concluded that a record of Google searches for a person's name or home address provided only innocuous information, insufficient to meet *Carpenter*'s intimacy prong.[25] But in *People v. Seymour*, the Colorado Supreme Court assessed the intimacy of search data in the abstract.[26] Specifically, the court reasoned that "online search history may indicate an individual's interest in a specific religion or research into sensitive medical conditions, information that could reveal intimate details about an individual's private life."[27] *Seymour* accordingly found search data sufficiently intimate to warrant protection under the Colorado Constitution.[28]

A court's choice whether to look to the intimacy of particular search terms requested by law enforcement—versus search history in the abstract—is likely decisive with respect to the intimacy prong. As Professor Orin Kerr notes, search data, as a category of information, clearly tends "to reveal a person's 'familial, political, professional,

available by the digital world. Second, generating the records must be unavoidable. And third, the information must be from the kinds of records that reveal the privacies of life.").

[23] See Commonwealth v. Kurtz, 294 A.3d 509, 522–23 (Pa. Super. Ct. 2023); People v. Seymour, 536 P.3d 1260, 1271–72 (Colo. 2023); Commonwealth v. Clements, 113 Va. Cir. 576, 587, 589 (2024).

[24] See *Kurtz*, 294 A.3d at 522 (looking to "the information provided by Google *here*," rather than search terms generally, to evaluate the intimacy of information revealed by a keyword warrant (emphasis added)).

[25] Id. at 522–23 (noting that the request "did not require production of data that shed light on Appellant's political views, health information, or other sensitive matters").

[26] See 536 P.3d at 1271.

[27] Id.

[28] Id. at 1272.

religious, and sexual associations.'"[29] But as *Kurtz* demonstrates, focusing on the records that investigators actually requested in the instant case will likely yield the opposite conclusion, given that law enforcement typically asks for relatively innocuous search terms.[30] This split over particularized versus categorical intimacy analysis is not limited to the context of search data—it plagues the post-*Carpenter* Fourth Amendment privacy framework.[31] Until the Supreme Court weighs in, courts applying *Carpenter* to search data are likely to diverge.

Next, consider *Carpenter*'s voluntariness prong. Perhaps buttressing commentators' observations that *Carpenter* has not been interpreted in a uniform way,[32] only one of the three courts addressing search data inquired into the voluntariness of its third-party exposure. *Kurtz* reasoned that *Carpenter*'s involuntary exposure prong was not met because "[b]y typing in his search query into the search engine and pressing enter, [Kurtz] affirmatively turned over the contents of his search to Google, a third party, and voluntarily relinquished his privacy interest in the search."[33] *Kurtz*'s conclusion is plausible enough: entering search queries is, after all, a voluntary act. However, some courts read *Carpenter*'s conception of voluntariness in a more nuanced way, asking whether the technology at issue is "indispensable to participation in modern society,"[34] which renders third-party exposure functionally involuntary.[35]

[29] Kerr, Digital Fourth Amendment, supra note 15, at 169 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018)).

[30] See *Kurtz*, 294 A.3d at 517 (victim's name and home address); *Seymour*, 536 P.3d at 1268 (address of targeted house); Commonwealth v. Clements, 113 Va. Cir. 576, 587 (2024) (victim's home address).

[31] Compare Paul Ohm, The Many Revolutions of *Carpenter*, 32 Harv. J.L. & Tech. 357, 378 (2019) ("*Carpenter* . . . should be applied not necessarily to the specific facts of a case but rather to the *category of information* being sought." (emphasis added)), with United States v. Castellanos, No. 21-cr-00348, 2023 WL 2466789, at *8 (N.D. Ga. Feb. 17, 2023) ("*Carpenter* should not be extended categorically to all real-time CSLI. . . . [W]hether a Fourth Amendment violation has occurred instead depends on how much data was captured and for how long, and more importantly, what the data reveals about an individual's location and movements." (footnote omitted)).

[32] See Ohm, supra note 31, at 370 (predicting that there will be "disagreement about the precise list of *Carpenter* factors"); Matthew Tokson, The Aftermath of *Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021, 135 Harv. L. Rev. 1790, 1793 (2022) ("Scholars disagree sharply about whether *Carpenter* implicitly created such a test, and if so, what that test requires.").

[33] *Kurtz*, 294 A.3d at 522.

[34] *Carpenter*, 138 S. Ct. at 2210.

[35] See United States v. Chatrie, 136 F.4th 100, 127 (4th Cir. 2025) (mem.) (Wynn, J., concurring in the judgment) (reasoning that "[s]haring Location History . . . is not

Yet as applied to search data, this more nuanced conception of *Carpenter*'s voluntariness prong fails to produce a clear answer. Professor Kerr is unsure how courts should resolve the social indispensability question because, for some people, "searching is like breathing," while others "may feel perfectly able to participate in modern society without searching all that often or even at all."[36] Judicial intuitions will undoubtedly differ, and courts could reasonably apply *Carpenter*'s voluntary exposure principle to reach contradictory conclusions.

Given the indeterminacy of *Carpenter*'s doctrinal framework, courts assessing search data under the Fourth Amendment's privacy rubric are unlikely to reach uniform results. Some will require a warrant to access search data while others will not. Such an uneven landscape will create uncertainty for police officers and leave members of the public wondering whether their search data is protected, thus frustrating core Fourth Amendment values: clarity and uniformity.[37] Accordingly, courts considering law enforcement requests for search data would do well to consider an alternative path. Fortunately, "[t]here is another way."[38]

II. A PATH FORWARD: THE *JONES* TRESPASS TEST

Since the Founding, it has been understood that physical trespass onto a constitutionally protected area—persons, houses, papers, and effects—with the intent to obtain information is a search.[39] To be sure, *Katz*'s injection of privacy into Fourth Amendment search analysis led many courts and litigants to view privacy, rather than property interests, as the

meaningfully voluntary" because "Americans face enormous pressure to entrust detailed personal information to third parties in exchange for services" (citing *Carpenter*, 138 S. Ct. at 2220)).

[36] Kerr, Digital Fourth Amendment, supra note 15, at 170.

[37] See Dunaway v. New York, 442 U.S. 200, 213–14 (1979) ("A single, familiar standard is essential to guide police officers . . . ."); Atwater v. City of Lago Vista, 532 U.S. 318, 347 (2001) (noting that Fourth Amendment rules should "respect the values of clarity and simplicity").

[38] *Carpenter*, 138 S. Ct. at 2267 (Gorsuch, J., dissenting).

[39] See United States v. Jones, 565 U.S. 400, 405 (2012) (observing that the Court's "Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century"); Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 816 (2004) [hereinafter Kerr, New Technologies] ("[E]arly courts interpreted the Fourth Amendment as a claim against government interference with property rights, and in particular, rights against trespass.").

appropriate gauge of Fourth Amendment protection.[40] But in 2012, the Court revived the trespass test. *United States v. Jones* explained that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test" and found that a search occurred when police officers placed a GPS tracker on the outside of Jones's Jeep.[41] The Court reaffirmed the viability of the trespass test in *Florida v. Jardines*, finding that the police conducted a search when they walked onto the suspect's porch with a drug-sniffing dog.[42]

Justice Gorsuch, dissenting in *Carpenter*, called for applying this physical trespass test to digital information.[43] According to Justice Gorsuch, the trespass test does not distinguish between physical and digital property because traditional Fourth Amendment analysis simply "asked if a house, paper or effect was *yours* under law. No more was needed to trigger the Fourth Amendment."[44] For Justice Gorsuch, it seemed "entirely possible a person's cell-site data could qualify as *his* papers or effects under existing law," such that its inspection by law enforcement amounted to a Fourth Amendment trespass search.[45]

Like Justice Gorsuch argued in relation to CSLI, we argue that courts should apply the trespass test to search data.[46] At least two reasons justify this approach. First, the trespass test provides certainty in future cases. Where *Katz* and *Carpenter* take courts down muddled doctrinal paths that lead to conflicting results, the trespass test produces a clear answer: accessing search data is always a search.[47] This bright-line rule will

[40] See Kiel Brennan-Marquez & Andrew Tutt, Offensive Searches: Toward a Two-Tier Theory of Fourth Amendment Protection, 52 Harv. C.R.-C.L. L. Rev. 103, 114 (2017) ("The common wisdom, at least until *Jones*, was that the '*Katz* test' . . . operates as both a floor and a ceiling; and that it constitutes the sole test for determining whether the Fourth Amendment governs police conduct.").

[41] *Jones*, 565 U.S. at 403–05, 409.

[42] 569 U.S. 1, 8 (2013). To be sure, *Jones* and *Jardines* articulated somewhat different standards. Compare *Jones*, 565 U.S. at 405 ("common-law trespass"), with *Jardines*, 569 U.S. at 7 ("unlicensed physical intrusion"). However, despite the differing articulations, we assume that *Jardines* did not alter *Jones*'s common law trespass test. See infra note 133.

[43] See *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).

[44] Id. at 2267–68.

[45] Id. at 2272.

[46] The dissenting Justices in *People v. Seymour* share our view. See People v. Seymour, 536 P.3d 1260, 1285 (Colo. 2023) (Marquez, J., dissenting, joined by Samour, J.) ("[T]he government-directed scan of Seymour's Google search history for particular keywords constituted a Fourth Amendment 'search.' In other words, law enforcement's digital entry into Seymour's search history constituted a trespass on his digital property.").

[47] See infra Section II.C.

streamline judicial treatment of requests for search data and provide valuable clarity for citizens and law enforcement. Professor Michael O'Connor cites certainty as a virtue of the trespass test, noting that "[b]y shifting the focus from privacy to property, the contours of [Fourth Amendment protection] should stabilize earlier and more firmly than under *Katz*."[48]

Second, the trespass test naturally incorporates positive law,[49] allowing democratically elected legislatures to help define the breadth of the Fourth Amendment.[50] Legislative input is particularly helpful in crafting Fourth Amendment rules related to rapidly evolving technology, such as search data.[51] As Professor Kerr explains, the judiciary's capacity to quickly respond to the impact of technological development on citizens is necessarily limited, and therefore "the legislative branch rather than the judiciary should create the primary investigative rules when technology is changing."[52]

To be sure, the idea that government inspection of digital information held on third-party servers is a search under the traditional trespass test may seem somewhat counterintuitive.[53] Indeed, no member of the Court joined Justice Gorsuch's *Carpenter* dissent. However, this Part demonstrates that current law supports finding a Fourth Amendment trespass search when law enforcement accesses search data.

The Court has repeatedly emphasized that the trespass test is rooted in the text of the Fourth Amendment,[54] which makes clear that if a house,

[48] Michael J. O'Connor, Digital Bailments, 22 U. Pa. J. Const. L. 1271, 1275 (2020).

[49] See infra Section II.A.

[50] See William Baude & James Y. Stern, The Positive Law Model of the Fourth Amendment, 129 Harv. L. Rev. 1821, 1852 (2016) ("The positive law model carves out significant room for legislative participation in the Fourth Amendment context.").

[51] See Riley v. California, 573 U.S. 373, 408 (2014) (Alito, J., concurring in part and concurring in the judgment) ("Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.").

[52] Kerr, New Technologies, supra note 39, at 806.

[53] See Orin S. Kerr, The Two Tests of Search Law: What is the *Jones* Test, and What Does That Say About *Katz*?, Wash. U. L. Rev. (forthcoming 2025) (manuscript at 36) [hereinafter Kerr, Two Tests], https://papers.ssrn.com/sol3/papers.cfm?abstract_id=5129549 [https://perma.cc/EY92-4YJT] ("[T]he Fourth Amendment implications of digital trespass should be answered under *Katz* rather than *Jones*.").

[54] See United States v. Jones, 565 U.S. 400, 405 (2012) ("The text of the Fourth Amendment reflects its close connection to property . . . ."); Florida v. Jardines, 569 U.S. 1, 5 (2013) (stating that the text of the Fourth Amendment "establishes [the trespass test as] a simple baseline").

paper, or effect is yours, you have an interest in its protection from unreasonable search and seizure.[55] Accordingly, we justify its application to search data by reference to that text. Specifically, we argue that law enforcement access to search data is a trespass search if three questions can be answered in the affirmative. First, can search engine users claim that search data is "theirs" within the meaning of the Fourth Amendment? Second, is search data a Fourth Amendment "paper"? Third, does government inspection of search data amount to a *Jones* trespass? This Part explains why the answer to all three questions is yes.

A. Is Search Data "Yours" Within the Meaning of the Fourth Amendment?

The Fourth Amendment protects the "right of the people to be secure in *their* persons, houses, papers, and effects."[56] No one disputed that Antoine Jones's car was *his*.[57] And Joelis Jardines's porch was clearly *his* property.[58] But it is less apparent whether search data, which is held on a search engine's servers, belongs to the user. In his *Carpenter* dissent, Justice Gorsuch acknowledged that Fourth Amendment ownership analysis is underdeveloped—the Supreme Court has not yet identified the appropriate source of Fourth Amendment property rights nor stated what property interest is sufficient to establish Fourth Amendment ownership.[59] We take the position that an individual owns an item in the Fourth Amendment sense when current positive law[60] grants them a right to exclude others from that item.

Though scholars have suggested alternatives,[61] we adopt Professor O'Connor's persuasive argument that current positive law is the proper

[55] See U.S. Const. amend. IV.

[56] Id. (emphasis added).

[57] *Jones*, 565 U.S. at 404 n.2.

[58] *Jardines*, 569 U.S. at 5–6.

[59] See Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting) ("[W]hat kind of legal interest is sufficient to make something *yours*? And what source of law determines that?"); see also Byrd v. United States, 584 U.S. 395, 412 (2018) (Thomas, J., concurring) ("[W]hat body of law determines whether [a Fourth Amendment] property interest is present—modern state law, the common law of 1791, or something else?").

[60] Black's Law Dictionary defines positive law as "the codes, statutes, and regulations that are applied and enforced in the courts." Positive Law, Black's Law Dictionary (8th ed. 2004).

[61] See Morgan Cloud, Property Is Privacy: Locke and Brandeis in the Twenty-First Century, 55 Am. Crim. L. Rev. 37, 44–47, 71 (2018) (arguing that Fourth Amendment property interests should be determined by reference to Lockean natural rights); Danielle D'Onfro &

source of Fourth Amendment property interests.[62] Relying on positive law to help define the scope of Fourth Amendment protections aligns with Supreme Court precedent,[63] has a basis in history,[64] and enjoys widespread support in legal scholarship.[65] Moreover, as Professor O'Connor explains, looking to positive law to determine Fourth Amendment ownership is consistent with the Court's Takings and Due Process Clause cases, which have consistently identified positive law as the source of property interests.[66] Accordingly, we embrace Professor O'Connor's conclusion that "the Fourth Amendment should respect property rights as defined by legislatures,"[67] in no small part because Justice Scalia, the author of *Jones* and *Jardines*, endorsed such an approach in his *Georgia v. Randolph* dissent.[68]

Still, identifying positive law as the proper source of Fourth Amendment property rights is only half the battle. As Justice Gorsuch noted in *Carpenter*, the Court has not yet defined what type of property interest is sufficient to make something "yours" within the meaning of the Fourth Amendment.[69] One might be tempted to read "their" to include only property that a person presently possesses. Some of the Court's Fourth Amendment "standing" cases might seem to support such a view. For example, *Rawlings v. Kentucky* held that Rawlings lacked Fourth Amendment protection in his property because he had relinquished

Daniel Epps, The Fourth Amendment and General Law, 132 Yale L.J. 910, 914 (2023) (arguing that the Fourth Amendment recognizes property interests arising out of general law).

[62] See O'Connor, supra note 48, at 1278–82.

[63] See, e.g., Florida v. Riley, 488 U.S. 445, 451 (1989) ("[I]t is of obvious importance that the helicopter in this case was *not* violating the law . . . .").

[64] See Orin S. Kerr, Four Models of Fourth Amendment Protection, 60 Stan. L. Rev. 503, 516 (2007) ("The positive law model has deep roots in Fourth Amendment history.").

[65] See Baude & Stern, supra note 50, at 1825–26; Richard M. Re, The Positive Law Floor, 129 Harv. L. Rev. F. 313, 332 (2016) (proposing a variation on Baude and Stern's model); Laura K. Donohue, Functional Equivalence and Residual Rights Post-*Carpenter*: Framing a Test Consistent with Precedent and Original Meaning, 2018 Sup. Ct. Rev. 347, 354 (2019) ("Positive law . . . may prove probative in regard to the existence of a property right: where federal or state law has *acknowledged a property right* and placed a correlative *duty of noninterference* on others, government intrusions may constitute a search or seizure within the meaning of the Fourth Amendment.").

[66] O'Connor, supra note 48, at 1283–85.

[67] Id. at 1280.

[68] 547 U.S. 103, 144 (2006) (Scalia, J., dissenting) ("We have consistently held that 'the existence of a property interest is determined by reference to existing rules or understandings that stem from an independent source such as state law.'" (internal quotation marks omitted) (quoting Phillips v. Wash. Legal Found., 524 U.S. 156, 164 (1998))).

[69] Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

possession by placing it in his companion's purse.[70] But *Rawlings* merely stands for the proposition that individuals may lack a *reasonable expectation of privacy* in property they do not presently possess.[71] Fourth Amendment protections under the *trespass* test are untethered to privacy expectations.[72] Accordingly, cases decided under the *Katz* rubric, like *Rawlings*, have no bearing on what kind of property interest is sufficient to establish Fourth Amendment protection.

Justice Gorsuch, for one, doubts that "exclusive control of property is always a necessary condition to the assertion of a Fourth Amendment right."[73] The Court's pre-*Katz* cases support Justice Gorsuch's view. In *Ex Parte Jackson*, the Court held that the police may not intercept a letter in the mail and examine its contents without a warrant.[74] The Court reasoned that the Fourth Amendment right "to be secure in [one's] papers against unreasonable searches and seizures extends to their papers . . . *wherever they may be*."[75] And in *Weeks v. United States*, the Court found a search occurred when police examined letters in the defendant's home, even though the defendant lacked possession of those letters at the time of the search.[76] *Ex Parte Jackson* and *Weeks* thus confirm that property can be "yours" under the Fourth Amendment even if you do not currently possess it.

Rather than requiring a present possessory interest, we argue that Professor O'Connor is correct to identify the right to exclude as the property interest that makes something "yours" for Fourth Amendment purposes.[77] In explaining the centrality of the right to exclude, Professor O'Connor undertakes an extensive survey of Fourth Amendment history and case law.[78] We need not rehash those arguments here. Instead, we simply point out that equating a positive law right to exclude with Fourth Amendment ownership is analytically consistent with the trespass test. A

[70] 448 U.S. 98, 104–06 (1980).

[71] See id. at 105 ("[Rawlings] had no subjective expectation that [his companion's] purse would remain free from governmental intrusion . . . .").

[72] See *Carpenter*, 138 S. Ct. at 2268 (Gorsuch, J., dissenting) (observing that the trespass test is not "hobbled by" *Katz* and its progeny).

[73] Id. at 2269.

[74] 96 U.S. 727, 733 (1877).

[75] Id. (emphasis added).

[76] 232 U.S. 383, 393 (1914).

[77] See O'Connor, supra note 48, at 1290 ("A Fourth Amendment property right arises when an owner may generally exclude others from a person, house, paper, or effect." (emphasis omitted)).

[78] See id. at 1286–91.

trespass is, at bottom, a violation of a person's right to exclude.[79] Accordingly, it makes intuitive sense for the right that renders the trespass test applicable to be the same right that the tort of trespass protects.

Professor O'Connor takes the important step of discussing how current positive law might grant individuals a right to exclude others from digital information held on third-party servers.[80] Specifically, he argues that the Stored Communications Act ("SCA"), in some cases, supplies such an exclusion right in digital data.[81] However, Professor O'Connor does not address whether the SCA, whose application is highly context-dependent,[82] grants an exclusion right in search data specifically. Accordingly, we build on Professor O'Connor's work by explaining why the SCA grants search engine users a Fourth Amendment-triggering right to exclude others from their search data. In other words, users "own" their search data within the meaning of the Fourth Amendment because current positive law—the SCA—grants them a right to exclude others from it.[83]

1. Stored Communications Act

Section 2702(a) of the SCA broadly prohibits public providers of communication and computing services from voluntarily disclosing

[79] See Munger v. Seehafer, 890 N.W.2d 22, 33–34 (Wis. Ct. App. 2016) ("The true 'injury' produced by an intentional trespass is the violation of the possessor's right to exclude others . . . ."); see also infra Section II.C.

[80] See O'Connor, supra note 48, at 1291–1306.

[81] See id. at 1305–06.

[82] See Hately v. Watts, 917 F.3d 770, 790 (4th Cir. 2019).

[83] We are not the first to suggest that search engine users retain a Fourth Amendment-triggering property interest in their search data. See Dalia Wrocherinsky, Comment, Finding Rights in the Fine Print: How Terms of Services Agreements Can Turn Consumer Search History into Digital Property, 14 Am. U. Bus. L. Rev. 501, 519–23 (2024) (arguing that search engine terms of service grant users a Fourth Amendment property right in their search data). However, Wrocherinsky's argument is ultimately untenable because it draws a property right, which binds "the rest of the world," from a private contract, which "bind[s] only the parties to the [contract]." Thomas W. Merrill & Henry E. Smith, The Property/Contract Interface, 101 Colum. L. Rev. 773, 776–77 (2001). Because terms of service determine the rights and obligations as between only the user and the search engine, Professor Kerr concludes that these private agreements "cannot create Fourth Amendment Rights." Orin S. Kerr, Terms of Service and Fourth Amendment Rights, 172 U. Pa. L. Rev. 287, 328 (2024) [hereinafter Kerr, Terms of Service]; id. at 290 (explaining that "[t]he Fourth Amendment provides rights against the government," whereas Terms of Service "define legal relationships between private parties"). Our approach is more doctrinally sound because it grounds the exclusion right in a positive law source that imposes a duty of noninterference on the entire world rather than a single private entity. See infra Subsection II.A.1.

certain user information to third parties.[84] The Act adds teeth to this prohibition by granting a civil cause of action to any "person aggrieved by any violation of [the SCA]," provided the violation was committed "with a knowing or intentional state of mind."[85] Accordingly, if a provider knowingly and voluntarily shares user information in violation of the SCA, the user may sue the provider.[86] In effect, this cause of action means that users of certain online services have a statutory right to exclude others from accessing their information, enforceable against the provider who made such access possible.[87] As Professor O'Connor puts it, the SCA's private cause of action "grant[s] a broad right to exclude [that] courts should treat . . . as a Fourth Amendment property right."[88] Courts as well have interpreted the SCA as creating a property right. For example, in *Theofel v. Farey-Jones*, the U.S. Court of Appeals for the Ninth Circuit recognized that the SCA safeguards individuals' "proprietary interests," reasoning that the SCA protects user information held by providers "[j]ust as trespass protects those who rent space from a commercial storage facility to hold sensitive documents."[89] Thus, the SCA is a viable positive law source of a right to exclude.

But does the Act cover the voluntary disclosure of search data by search engine companies? The SCA's prohibition on voluntary disclosure only applies to providers of "electronic communication service[s]" ("ECS") or "remote computing service[s]" ("RCS").[90] Under the statute, an ECS "provides to users . . . the ability to send or receive wire or electronic communications,"[91] whereas an RCS provides "computer storage or processing services by means of an electronic communications system" to the public.[92] Importantly, the ECS/RCS distinction is context-dependent and focuses on the function a provider performs at a given time

[84] 18 U.S.C. § 2702(a).

[85] Id. § 2707(a).

[86] See In re Zynga Priv. Litig., 750 F.3d 1098, 1105 n.5 (9th Cir. 2014) (holding that private plaintiffs had standing to sue providers that allegedly shared the plaintiffs' information in violation of the SCA); see also infra note 107 (further addressing the nuances in the SCA's private cause of action).

[87] See Walker v. Coffey, 956 F.3d 163, 167 (3d Cir. 2020) (characterizing the SCA as "prohibit[ing] certain forms of electronic trespass").

[88] O'Connor, supra note 48, at 1306.

[89] 359 F.3d 1066, 1072 (9th Cir. 2004).

[90] 18 U.S.C. § 2702(a).

[91] Id. § 2510(15).

[92] Id. § 2711(2).

rather than the provider's general status.[93] Courts have yet to address whether search engines qualify as an ECS or RCS.

Search engine companies are properly characterized as RCS providers because they process and then store user search queries for the user's later use.[94] When users permit Google to retain their search data, Google processes search query information to provide a more customized user experience.[95] Additionally, Google's storage of search data allows users to revisit their old queries, effectively functioning like a "virtual filing cabinet," which courts treat as governed by the RCS rule.[96] Given that mainstream search engines deliver services "to the public,"[97] a typical search engine functions as an RCS under the SCA.[98]

The applicability of the SCA's voluntary disclosure prohibition, however, depends on the type of information at issue.[99] While the SCA permits disclosure of "record" or "subscriber" information to private parties,[100] no such exception applies to the "contents of a communication."[101] Under the SCA, "contents" are defined as "information concerning the substance, purport, or meaning of [any electronic communication]."[102] Courts have yet to directly address whether search data is content or non-content information under the SCA.

[93] Orin S. Kerr, A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It, 72 Geo. Wash. L. Rev. 1208, 1215–16 (2004).

[94] Google appears to hold itself out as an RCS. See Google's Opposition to the Government's Motion to Compel at 19–20, Gonzales v. Google, 234 F.R.D. 674 (N.D. Cal. 2006) (No. 06-cv-80006).

[95] See Find & Control Your Web & App Activity, Google, https://support.google.com/websearch/answer/54068?hl=en&co=GENIE.Platform [https://perma.cc/UU4T-QFH8] (last visited Aug. 3, 2025) (giving users the option to allow Google to retain search data); id. (noting that data retention permits Google to provide "more personalized experiences").

[96] See Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901–02 (9th Cir. 2008) (reasoning that a remote computing service is akin to a "virtual filing cabinet").

[97] 18 U.S.C. § 2711(2); see also Andersen Consulting LLP v. UOP, 991 F. Supp. 1041, 1042 (N.D. Ill. 1998) (defining "public" as "'the 'aggregate of the citizens' or 'everybody'" (quoting Public, Black's Law Dictionary (6th ed. 1990))).

[98] But see Matthew A. Goldberg, Comment, The Googling of Online Privacy: Gmail, Search-Engine Histories and the New Frontier of Protecting Private Information on the Web, 9 Lewis & Clark L. Rev. 249, 261–62 (2005) (arguing that search engines should qualify as ECS providers).

[99] See 18 U.S.C. § 2702(b)–(c).

[100] Id. § 2702(c)(6) (permitting disclosure of record information to "any person other than a governmental entity").

[101] See generally id. § 2702(b).

[102] Id. § 2510(8).

However, courts have, in dicta, suggested the former.[103] And intuitively, search queries should count as "content" information because they contain the "substance"[104] of electronic communications transmitted from the user to the search engine. Thus, in the absence of a case-specific exception,[105] search engines violate the SCA if they knowingly and voluntarily disclose a user's search queries to a private party.[106] Given that the SCA grants users a civil cause of action to enforce such violations,[107] the Act plainly affords search engine users a statutory right to exclude third parties from their search data.[108]

The fact that the SCA permits disclosure of content information to law enforcement[109] does not strip search engine users of their property right to exclude. In the Due Process context, the Court has held that the government cannot legitimately grant a property right while exempting itself from having to comply with that property right.[110] While the

[103] See In re Zynga Priv. Litig., 750 F.3d 1098, 1108–09 (9th Cir. 2014) ("Under some circumstances, a user's request to a search engine for specific information could constitute a communication such that divulging a URL containing that search term to a third party could amount to disclosure of the contents of a communication."); In re Subpoena 2018R00776, 947 F.3d 148, 152 (3d Cir. 2020) (suggesting that "search histories" count as "content" information).

[104] 18 U.S.C. § 2510(8).

[105] See id. § 2702(b)(1)–(9).

[106] Id. § 2702(a)(2).

[107] The plain text of 18 U.S.C. § 2707(a) grants a civil cause of action to individuals "aggrieved by any violation" of the SCA, which seems to include violations of § 2702(a)(2)'s RCS voluntary disclosure prohibition. Id. § 2707(a). However, some authorities suggest that § 2707(a)'s cause of action is limited to violations of § 2701(a)'s unauthorized access provision, which only applies to ECS providers. See James G. Carr, Patricia L. Bellia & Evan A. Creutz, 2 Law of Electronic Surveillance § 8:57 (2025). Still, the balance of authorities maintains that a § 2702(a)(2) violation provides grounds for a § 2707(a) civil suit. See *In re Zynga*, 750 F.3d at 1104–05, 1109 (contemplating a civil suit against an RCS provider under § 2707(a) for violation of § 2702(a)(2)'s RCS rule, but resolving the case on separate grounds); Charles Doyle, Cong. Rsch. Serv., R41734, Privacy: An Abridged Overview of the Electronic Communications Privacy Act 7 (2012) ("RCS providers . . . may be liable for civil damages . . . under section 2707 for any violation of section 2702.").

[108] Cf. James Y. Stern, Property's Constitution, 101 Calif. L. Rev. 277, 286–87 (2013) ("The existence of a property right does not depend simply on whether some other body of law uses the term 'property' or declares that a person has a 'property right.'").

[109] See 18 U.S.C. § 2703(b)(1) (providing that, if certain law enforcement-related procedural steps are followed, "[a] governmental entity may require a provider of remote computing service to disclose the contents of any wire or electronic communication"); id. § 2702(b)(2) (incorporating Section 2703's law enforcement exception by reference).

[110] See Cleveland Bd. of Educ. v. Loudermill, 470 U.S. 532, 541 (1985) ("'Property' cannot be defined by the procedures provided for its deprivation . . . . ['] While the legislature may elect not to confer a property interest . . . , it may not constitutionally authorize the deprivation

Supreme Court has yet to apply this principle in the Fourth Amendment context, Justice Gorsuch's questioning at oral argument in *Carpenter* indicates his (and the government's) understanding that "the government [cannot] acknowledge a property right but then strip it of any Fourth Amendment protection."[111] In short, the right to exclude conferred by the SCA is, for Fourth Amendment purposes, as good against the government as it is against any private individual.[112]

B. Is Search Data a Fourth Amendment "Paper"?

Merely owning an item does not necessarily mean that law enforcement trespass on that property amounts to a search. The Fourth Amendment does not protect all property.[113] Instead, the text of the Amendment "embod[ies] a particular concern for government trespass upon the areas ('persons, houses, papers, and effects') it enumerates."[114] Accordingly, the trespass test only protects search data if it falls into one of these categories of constitutionally protected property. This Section identifies three reasons why courts should treat search data as a Fourth Amendment paper.[115] First, the expressive nature of search data aligns with the Fourth Amendment's historical role in protecting First Amendment material. Second, and relatedly, treating search data as a

of such an interest, once conferred, without appropriate procedural safeguards.'" (quoting Arnett v. Kennedy, 416 U.S. 134, 167 (1974) (Powell, J., concurring in part and concurring in the judgment in part) (footnote omitted))).

[111] Transcript of Oral Argument at 57, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402); cf. Baude & Stern, supra note 50, at 1825–26 ("Fourth Amendment protection . . . is warranted when government officials either violate generally applicable law or *avail themselves of a governmental exemption from it*." (emphasis added)).

[112] See O'Connor, supra note 48, at 1301 ("[W]hen the Government grants a property right, exempting itself from that property right seems unconstitutional.").

[113] See Myers v. Town of Elkton, 745 F. Supp. 3d 219, 232 (D. Md. 2024) ("Whether a particular area is 'constitutionally protected' does not necessarily align with property boundaries.").

[114] United States v. Jones, 565 U.S. 400, 406 (2012) (quoting U.S. Const. amend. IV).

[115] We do not consider the possibility that search data might constitute a Fourth Amendment "effect," in part because the definition of "effect" is radically underdeveloped. See Maureen E. Brady, The Lost 'Effects' of the Fourth Amendment: Giving Personal Property Due Protection, 125 Yale L.J. 946, 957 (2016) (noting that, at least until *Jones*, "effects" received "little sustained attention from the Supreme Court"). Yet, it is notable that Justice Scalia, when asked at a Q-and-A event whether computer data could be an "effect," was reportedly impressed by the question. See Debra Cassens Weiss, Does Fourth Amendment Protect Computer Data? Scalia Says It's a Really Good Question, A.B.A. J. (Mar. 24, 2014, 1:06 PM), https://www.abajournal.com/news/article/asked_about_nsa_stuff_scalia_says_conversations_arent_protected_by_fourth_a [https://perma.cc/Z54S-EMJG].

Fourth Amendment paper is necessary to maintain the Amendment's Founding-era level of protection. Third, modern courts have invoked both of these rationales to treat various kinds of digital information as Fourth Amendment papers.

To begin, consider why the Fourth Amendment protects papers. The Framers recognized that warrantless searches of papers could chill First Amendment expressive and associational activity.[116] Indeed, the Supreme Court has noted that the Fourth Amendment was historically understood as a guardian of First Amendment freedoms.[117] As Michael Price of the Brennan Center points out, "[t]he history of the Fourth Amendment reveals a long and storied relationship between the right to be free from unreasonable searches and seizures and the principles of free speech now enshrined in the First Amendment."[118] Therefore, "'papers' should be read to protect expressive and associational data, regardless of its form, how it is created, or where it is located. . . . [Constitutional papers] may be digital files stored on a cell phone, hosted in 'the cloud,' or even generated by a third party."[119]

Search data implicates First Amendment freedoms no less than physical papers. Price makes the uncontroversial point that digital data "is quite capable of revealing information about one's political or religious associations, interests and dislikes, or habits and predilections that would otherwise be difficult to determine."[120] Indeed, search data, as compared to other types of digital information, bears particularly strongly on the First Amendment. The Colorado Supreme Court in *People v. Seymour* recognized that searching on the internet is an "expressive activity" because the internet "is a place where a citizen can explore ideas, receive information, and discover myriad perspectives on every topic

[116] See Marcus v. Search Warrant, 367 U.S. 717, 729 (1961) (noting the Framers' belief that "suppression of innocent expression inhered in the discretion confided in the officers authorized to exercise the power [of search and seizure]"); see also Stanford v. Texas, 379 U.S. 476, 482 (1965) (observing that general warrants were "systematically used" in "enforcing the laws licensing the publication of literature and, later, in prosecutions for seditious libel").

[117] See *Marcus*, 367 U.S. at 729 ("[The Fourth Amendment] was fashioned against the background of knowledge that unrestricted power of search and seizure could also be an instrument for stifling liberty of expression.").

[118] Michael W. Price, Rethinking Privacy: Fourth Amendment "Papers" and the Third-Party Doctrine, 8 J. Nat'l Sec. L. & Pol'y 247, 250 (2016).

[119] Id. at 249.

[120] Id. at 275.

imaginable."[121] Professor Neil Richards likewise argues that "[i]ntellectual records"—such as "terms entered into a search engine—are in a very real sense a partial transcript of the operation of a human mind. They implicate the freedom of thought and the freedom of intellectual exploration."[122] Accordingly, search data should be treated as a constitutional paper so that the Fourth Amendment can continue to serve its First Amendment prophylactic role.

In addition to its expressive nature, search data is functionally equivalent to physical papers. Jim Harper of the Cato Institute observes that "[t]he same information about each American's life that once resided on paper and similar media in attics, garages, workshops, master bedrooms, sewing rooms, and desk drawers, now resides, digitized, in cell phones and similar electronic devices."[123] Given the Court's emphasis on construing the Fourth Amendment to provide the level of protection that existed at the Founding,[124] this functional equivalence cuts in favor of treating search data as a constitutional paper. The similarity between library and bookstore records in 1791 and search data today means that failing to recognize search data as a constitutional paper would leave the Fourth Amendment with *less* textual coverage than it had at the Founding.[125] Such a construction would render the Amendment inappropriately under-protective.

With the history of constitutional papers and the need to conform Fourth Amendment construction to changing technology in mind, it is unsurprising that jurists have treated various types of digital data as Fourth Amendment papers. Justice Gorsuch, dissenting in *Carpenter*, suggested that CSLI data could count as a "modern-day paper[]."[126] Justice Kennedy, also in dissent, agreed that electronic information might

[121] People v. Seymour, 536 P.3d 1260, 1274 (Colo. 2023) (internal quotation marks omitted) (citation omitted).

[122] Neil M. Richards, Intellectual Privacy, 87 Tex. L. Rev. 387, 436 (2008).

[123] Jim Harper, Nat'l Const. Ctr., Administering the Fourth Amendment in the Digital Age 28 (2017), https://constitutioncenter.org/news-debate/special-projects/digital-privacy/the-fourth-amendment-in-the-digital-age [https://perma.cc/K5CK-8QHJ].

[124] See Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (construing the Fourth Amendment to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted" (alteration in original) (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001))).

[125] Cf. United States v. Rumely, 345 U.S. 41, 57 (1953) (Douglas, J., concurring) ("Once the government can demand of a publisher the names of the purchasers of his publications, . . . [f]ear of criticism goes with every person into the bookstall.").

[126] *Carpenter*, 138 S. Ct. at 2269 (Gorsuch, J., dissenting).

constitute a "modern-day equivalent[] of an individual's own 'papers.'"[127] Yet it is not just dissenters who have suggested digital information may be constitutional papers. The Sixth Circuit in *United States v. Warshak* analogized email to the physical letters that have been protected from warrantless search since the 1877 case *Ex Parte Jackson*, reasoning that "it would defy common sense to afford emails lesser Fourth Amendment protection" than "traditional forms of communication."[128] The Tenth Circuit in *United States v. Ackerman* took a similarly analogical approach. *Ackerman* acknowledged the parties' agreement that Ackerman's e-mails counted as a paper and added that "if opening and reviewing 'physical' mail is generally a 'search'— . . . why not 'virtual' mail too?"[129] The Ninth Circuit in *United States v. Cotterman* reached a similar conclusion but by purposive, rather than analogical, reasoning. Noting that papers were incorporated into the Fourth Amendment because they "reflect our most private thoughts and activities," *Cotterman* reasoned that digital information is the "type of material" that counts as a constitutional paper because it "contain[s] the most intimate details of our lives: financial records, confidential business documents, medical records and private emails."[130] Although these courts were addressing other kinds of digital information, their reasoning applies with equal force to search data.

In short, treating search data as a constitutional paper comports with the Fourth Amendment's historical role as a First Amendment prophylactic, renders the Fourth Amendment adequately protective in the digital age, and aligns with a growing body of precedent affording digital information constitutional paper status.

C. Is Law Enforcement Access to Search Data a Jones *Trespass?*

Concluding that search data is a user's Fourth Amendment paper is not, by itself, sufficient to show that law enforcement access to search data is

[127] Id. at 2230 (Kennedy, J., dissenting).

[128] United States v. Warshak, 631 F.3d 266, 285–86 (6th Cir. 2010).

[129] United States v. Ackerman, 831 F.3d 1292, 1304 (10th Cir. 2016) (first citing Ex Parte Jackson, 96 U.S. 727, 733 (1877); and then citing United States v. Van Leeuwen, 397 U.S. 249, 251 (1970)).

[130] United States v. Cotterman, 709 F.3d 952, 957, 964 (9th Cir. 2013).

a Fourth Amendment search. Rather, investigators must engage in some sort of trespass on the paper with an intent to gather information.[131]

To be sure, *Jardines* somewhat blurred the trespass test that *Jones* reincorporated into the Fourth Amendment. That is, *Jardines*, like *Jones*, rooted its analysis in property principles but avoided the word "trespass," focusing instead on whether the government engaged in an "unlicensed physical intrusion" of a constitutionally protected area.[132] Despite the different formulations, scholars generally agree that *Jones* and *Jardines* both endorsed some sort of trespass test.[133] But the question remains: What is the content of the trespass test set out in *Jones*? As Professor Kerr points out, lower courts have looked to various sources of law to fill in the trespass test.[134] Here, we take *Jones*'s reliance on "common-law trespass" at face value.[135] Although the precise contours of the common law trespass doctrine endorsed in *Jones* remain elusive,[136] Justice Alito's concurrence characterized common law trespass as requiring only "a violation of 'the dignitary interest in the inviolability of chattels.'"[137] But what would amount to such a violation? Given that commentators have recognized common law trespass as protecting property owners' "exclusive right to . . . use [their] property"[138] and common law courts

[131] A search occurred in *Jones* because the government trespassed on Jones's personal property "for the purpose of obtaining information." United States v. Jones, 565 U.S. 400, 404 (2012).

[132] Florida v. Jardines, 569 U.S. 1, 7 (2013).

[133] See Laurent Sacharoff, Constitutional Trespass, 81 Tenn. L. Rev. 877, 882 (2014) (arguing that *Jones* and *Jardines* "should be read to have created an express trespass test, despite *Jardines*' equivocation on this point"); D'Onfro & Epps, supra note 61, at 956 ("*Jones* and *Jardines* returned to trespass as an analytical starting point."). But see Kerr, Two Tests, supra note 53 (manuscript at 22) (arguing that both *Jones* and *Jardines* apply a physical intrusion test, rather than a trespass test).

[134] See Kerr, Two Tests, supra note 53 (manuscript at 2–3).

[135] *Jones*, 565 U.S. at 405 ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century."); see also id. at 406–07 (explaining that "*Katz* did not repudiate," but rather supplemented, the trespass approach to the Fourth Amendment); Kyllo v. United States, 533 U.S. 27, 31 (2001) (identifying that pre-*Katz* "Fourth Amendment jurisprudence" incorporated "common-law trespass" and citing cases).

[136] See Taylor v. City of Saginaw, 922 F.3d 328, 332 (6th Cir. 2019) ("*Jones* does not provide clear boundaries for the meaning of common-law trespass . . . .").

[137] *Jones*, 565 U.S. at 419 n.2 (Alito, J., concurring in the judgment) (quoting W. Page Keeton, Dan B. Dobbs, Robert E. Keeton & David G. Owen, Prosser and Keeton on the Law of Torts § 14, at 87 (5th ed. 1984)).

[138] Keeton et al., supra note 137, § 13, at 72.

have found liability for "mere touching,"[139] it is clear that a common law trespass was, at bottom, a violation of the property owner's right to exclude.[140] When investigators access someone's search data without permission, they violate that person's right to exclude and, accordingly, commit a common law trespass. Carried out with the intent to obtain information, such conduct amounts to a Fourth Amendment search.

Of course, common law trespass was concerned with *physical* invasions of property.[141] It might therefore seem that *virtually* inspecting someone's search data falls outside the scope of common law trespass. However, courts routinely find trespass liability even when the trespasser intermeddles with the owner's property through seemingly digital means.[142] How can this be? Lower courts have adopted the theory that unauthorized electronic access to digital information *does* indeed involve physical contact, albeit on a minute scale. For example, one district court reasoned that "the electronic signals sent by [the defendant] to retrieve information from [the plaintiff's] computer system are . . . sufficiently tangible to support a trespass cause of action."[143] Another recognized that "[e]lectronic signals generated and sent by computer have been held to be sufficiently physically tangible to support a trespass cause of action."[144] Accordingly, when law enforcement retrieves search data from the search engine's servers, the interplay of electrons between the computer systems supplies the requisite physicality.

[139] See W.V.H. Rogers, Winfield and Jolowicz on Tort 593 (16th ed. 2002); P.A. Landon, Pollock's Law of Torts: A Treatise on the Principles of Obligations Arising from Civil Wrongs in the Common Law 265 (15th ed. 1951) ("[C]ases are conceivable in which the power of treating a mere unauthorised touching as a trespass might be salutary and necessary . . . ."); see also William Leitch & Co. v. Leydon [1931] AC 90 (HL) 106 (Lord Blanesborough) (appeal taken from First Div. of the Ct. of Session in Scot.) (UK) ("The wrong to the appellants in relation to [the] trespass is constituted whether or not actual damage has resulted therefrom . . . ."); cf. United States v. Richmond, 915 F.3d 352, 358 (5th Cir. 2019) (concluding that the "act of tapping tires" with an investigatory purpose was a search under *Jones*).

[140] D'Onfro & Epps, supra note 61, at 956 ("Trespass is the tort that protects the right to exclude . . . .").

[141] See *Jones*, 565 U.S. at 404–05 ("We have no doubt that such a *physical* intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." (emphasis added)). But see State v. Wright, 961 N.W.2d 396, 416 (Iowa 2021) ("At the time of the founding, trespass was a broad concept that encompassed far more than physical intrusions into or on real or personal property." (citing 3 William Blackstone, Commentaries *208)).

[142] See United States v. Ackerman, 831 F.3d 1292, 1308 (10th Cir. 2016) (collecting cases).

[143] eBay, Inc. v. Bidder's Edge, Inc., 100 F. Supp. 2d. 1058, 1069 (N.D. Cal. 2000).

[144] Compuserve Inc. v. Cyber Promotions, Inc., 962 F. Supp. 1015, 1021 (S.D. Ohio 1997).

One might also think that law enforcement access to search data cannot amount to a cognizable trespass because merely copying and inspecting a user's search data inflicts no "harm" to the data. While it is true that modern tort law requires harm for an actionable trespass claim,[145] the common law imposed no such requirement.[146] This is why a search occurred in *Jones*, even though the credit-card-sized GPS inflicted no harm to Jones's Jeep.[147] As discussed above, the mere violation of a property owner's right to exclude was sufficient to establish a trespass at common law. Thus, the fact that investigators do no harm to the search data they examine is no bar to liability under the common law trespass test endorsed in *Jones*.

A final wrinkle remains. Accessing search data is a trespass only if done *without consent*.[148] One may therefore wonder, Do users give law enforcement permission to inspect their search data when they agree to search engine terms of service?[149] No.[150] Standard terms of service authorize search engines to disclose search data to investigators only in response to a valid warrant.[151] But perhaps more fundamentally, private contracts cannot generate consent for Fourth Amendment purposes. *Florida v. Jimeno* makes clear that Fourth Amendment consent requires

[145] See, e.g., Intel Corp. v. Hamidi, 71 P.3d 296, 302–03 (Cal. 2003) ("[O]ne who intentionally intermeddles with another's chattel is subject to liability only if his intermeddling is *harmful* to the possessor's materially valuable interest in the physical condition, quality, or value of the chattel . . . ." (emphasis omitted)).

[146] Justice Alito emphasized this distinction in his *Jones* concurrence, explaining that trespass to chattels could be maintained at common law for mere infringement on a "dignitary interest," as opposed to the "actual damage" that modern trespass doctrine requires. 565 U.S. at 419 n.2 (Alito, J., concurring in the judgment).

[147] Id. at 404–05 (majority opinion); id. at 405 ("[O]ur law holds the property of every man so sacred, that no man can set his foot upon his neighbour's close without his leave; if he does he is a trespasser, *though he does no damage at all* . . . ." (alteration in original) (emphasis added) (quoting Entick v. Carrington (1765) 95 Eng. Rep. 807, 817 (KB))).

[148] See Keeton et al., supra note 137, § 14, at 85 ("Thus it is a trespass . . . to make an *unpermitted* use of [chattel] . . . ." (emphasis added)).

[149] See Terms of Service: Information Requests, Google, https://policies.google.com/terms/information-requests [https://perma.cc/YV9T-B6P7] (last visited Aug. 3, 2025) (authorizing Google to share user information with certain third parties, including law enforcement).

[150] See Kerr, Terms of Service, supra note 83, at 328 (arguing that terms of service "have little or no impact on Fourth Amendment rights").

[151] See Terms of Service, supra note 149 (providing assurance that Google will only disclose user content data in response to a warrant); Frequently Asked Questions: Government Requests, Yahoo, https://www.yahooinc.com/transparency/about/faq-glossary.html [https://perma.cc/2J64-CU79] (last visited Aug. 3, 2025) (same).

an interaction with law enforcement.[152] Of course, such an interaction is lacking when a user signs up for an online service. Therefore, search engine terms of service do not give investigators permission to access search data without a warrant.[153]

We are not the first to recognize that a Fourth Amendment trespass search occurs when the government inspects digital information. In *United States v. Ackerman*, investigators read one of Ackerman's emails, which they had received from his email provider.[154] For the Tenth Circuit, that "seem[ed] pretty clearly to qualify as exactly the type of trespass to chattels that the [F]ramers sought to prevent when they adopted the Fourth Amendment."[155] The court emphasized that *Jones* embraced common law trespass principles to ensure that "the Fourth Amendment is no less protective of persons and property against governmental invasions than the common law was at the time of the founding."[156] Just as the Tenth Circuit applied common law trespass to law enforcement inspection of emails with an eye to the Fourth Amendment's guarantee of Founding-era protection, courts should do the same with respect to search data. As discussed in Section II.B, search data is the twenty-first-century equivalent of the written communications that were undoubtedly protected at the Founding.[157] To hold that the Fourth Amendment trespass test does not protect against government inspection of a functionally equivalent constitutionally protected area would contradict the Court's mandate that Fourth Amendment construction ought to "assure[] preservation of that degree of privacy against government that existed when the Fourth Amendment was adopted."[158]

In short, when law enforcement accesses search data, they commit a common law trespass onto a user's constitutional paper. When carried out

[152] 500 U.S. 248, 251 (1991) (asserting that the scope of Fourth Amendment consent is determined by asking, "[W]hat would the typical reasonable person have understood by the exchange between the officer and the suspect?").

[153] See United States v. DiTomasso, 56 F. Supp. 3d 584, 592 (S.D.N.Y. 2014) ("[I]t would subvert the purpose of the Fourth Amendment to understand its privacy guarantee as 'waivable' . . . [in a world where] the use of electronic devices almost always requires acquiescence to some manner of consent-to-search terms.").

[154] 831 F.3d 1292, 1294 (10th Cir. 2016).

[155] Id. at 1307.

[156] Id. (citing United States v. Jones, 565 U.S. 400, 405–06, 411 (2012)).

[157] See Entick v. Carrington, (1765) 19 How. St. Tr. 1029, 1066 ("Papers are the owner's . . . dearest property; and are so far from enduring a seizure, that they will hardly bear an inspection . . . .").

[158] Kyllo v. United States, 533 U.S. 27, 34 (2001).

with the intent to obtain information, such access amounts to a Fourth Amendment search.

III. IMPLICATIONS

Our trespass analysis in Part II suggests that individuals should receive Fourth Amendment protection for search data even though that data is possessed by a third party. Yet even after *Carpenter*, courts applying *Katz* routinely rely on the third-party doctrine to hold that no search occurs when law enforcement accesses digital information held by third parties.[159] The reader may wonder: Does our analysis challenge these holdings? In other words, would employing the *Jones* trespass test in the way we suggest uproot decades of third-party doctrine case law?[160] No. While not unfounded, this concern too quickly overlooks the limiting nuances of Fourth Amendment trespass analysis.

As Part II explains, the trespass test applies only when an individual (a) has a positive law right to exclude in (b) a constitutionally protected area. While search data satisfies both prongs, it is less clear that other types of data held on third-party servers would. Take ride-share records, for example. Ride-sharing companies like Uber and Lyft retain records of when and where customers are picked up and dropped off, and which roads they traveled.[161] This data was the subject of *Sanchez v. Los Angeles Department of Transportation*.[162] There, the Ninth Circuit relied on the third-party doctrine to hold that government collection of rentable e-scooter trip histories was not a search under *Katz*.[163] Though a complete Fourth Amendment trespass analysis of ride-share data is beyond the scope of this Essay, it suffices to point out that the trespass test would likely produce a result consistent with *Sanchez*.

[159] See, e.g., Speidell v. United States, 978 F.3d 731, 744 (10th Cir. 2020).

[160] To be sure, many would welcome an annihilation of the third-party doctrine. See, e.g., Neil Richards, The Third-Party Doctrine and the Future of the Cloud, 94 Wash. U. L. Rev. 1441, 1442 (2017) ("[T]he Third-Party Doctrine is manifestly unsuited to the protection of our digital civil liberties."). Yet the doctrine has its defenders. See Orin S. Kerr, The Case for the Third-Party Doctrine, 107 Mich. L. Rev. 561, 564–65 (2009) (arguing that critics have overlooked the benefits of the doctrine).

[161] See, e.g., Uber Privacy Notice: Riders and Order Recipients, Uber, https://www.uber.com/us/en/privacy-notice-riders-order-recipients/#data-we-collect [https://perma.cc/4VGZ-6H6K] (last visited Aug. 3, 2025).

[162] 39 F.4th 548, 552 (9th Cir. 2022).

[163] Id. at 561.

Begin by considering whether ride-share data would even qualify as a constitutional paper.[164] Search data captures users' thoughts and curiosities, but ride-share data merely reflects users' geographic drop-off and pickup locations. Accordingly, the First Amendment rationale that justified treating search data as a Fourth Amendment paper applies with much less force to ride-share data. Additionally, ride-share data lacks a readily apparent Founding-era analogue, thus eliminating the functional equivalence argument that we marshaled in support of treating search data as a Fourth Amendment paper. Given this lack of justification for affording ride-share data constitutional paper status, the trespass test may simply not apply to that type of digital information.

And even if ride-share data does count as a constitutional paper (or an effect, perhaps), ride-share users may lack a Fourth Amendment property interest in it. Recall that the SCA, the source of search engine users' property interest in their search data, permits disclosure of "record" information to private parties.[165] The SCA thus does not grant an exclusion right in ride-share location data, which courts have found to be "record" information.[166] While ride-share users may find a property right in some other source of positive law, their path to Fourth Amendment ownership is less clear than for search engine users.

Our point is not that ride-share data is necessarily unprotected by the trespass test. Rather, the preceding discussion merely points out that Fourth Amendment trespass analysis cannot simply be cut and pasted into new contexts because the applicability of the trespass test depends on the nature of the data at issue. Although the trespass analysis we endorse may, in some instances, find a search where *Katz* would not, it is unlikely to significantly upset settled Fourth Amendment doctrine.

CONCLUSION

Justice Gorsuch noted in his *Carpenter* dissent that "American courts are pretty rusty at applying the traditional [trespass] approach to the Fourth Amendment."[167] Government requests for search data are a

[164] See Price, supra note 118, at 271 ("[I]t is not immediately clear what kinds of data would fall under the aegis of Fourth Amendment 'papers.' ").

[165] 18 U.S.C. § 2702(c)(6).

[166] See, e.g., Gonzales v. Uber Techs., Inc., 305 F. Supp. 3d 1078, 1085 (N.D. Cal. 2018) ("Plaintiff's geolocation data is also record information rather than the content of a communication . . . ."); In re Carrier IQ, Inc., 78 F. Supp. 3d 1051, 1082–83 (N.D. Cal. 2015).

[167] Carpenter v. United States, 138 S. Ct. 2206, 2268 (2018) (Gorsuch, J., dissenting).

sensible place to start shaking off that rust. As this Essay explains, applying *Katz* to these requests produces muddled analysis and contradictory results, but trespass yields a clear answer: accessing search data is a Fourth Amendment search. By settling the threshold search question with respect to search data, this Essay adds urgency to the burgeoning dialogue over the constitutionality of reverse keyword warrants.[168] Whether keyword warrants satisfy the Fourth Amendment's probable cause and particularity requirements is, indeed, a debate worth having. Equally important, this Essay demonstrates how trespass principles can find a search where *Katz* may not, underscoring Justice Gorsuch's counsel that "[n]eglecting more traditional approaches may mean failing to vindicate the full protections of the Fourth Amendment."[169]

[168] See supra note 7.
[169] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).