YALE LAW & POLICY REVIEW

End-Running Warrants: Purchasing Data Under the Fourth Amendment and the State Action Problem

*Aaron X. Sobel**

"Every move you make, Every bond you break, Every step you take, I'll be watching you."[1]

Rather than obtain warrants, law enforcement and intelligence agencies now purchase mass datasets of precise geolocation information from third-party brokers. These location data reveal the most intimate aspects of our personal lives: our political beliefs, religious associations, sexual preferences, private activities, and much more. The limited scholarship on this topic suggests that whether the government must obtain a warrant to purchase these sensitive but commercially available data turns solely on whether users have a reasonable expectation of privacy in these records. But this Note suggests that this (albeit necessary) privacy analysis misses the crux of the controversy.

The Fourth Amendment regulates unreasonable government *action, yet privacy proponents and defenders of the practice alike have neglected to analyze whether a purchase is a government search that* independently *violates a reasonable expectation of privacy. This Note—the first comprehensive examination of data purchases under Fourth Amendment*

* J.D., Yale Law School, 2023. A.B., Princeton University, 2019. My deepest thanks to Professor Oona Hathaway for her extensive feedback, principled guidance, and steadfast mentorship. Thank you as well to Jonathan Fischbach for his brilliant engagement, thorough and constructive comments, and thoughtful counsel throughout the drafting process. Sincerest thanks to Amy Chua for her tireless advocacy, unrivaled compassion, and unwavering faith in me. And finally, to the incredibly thoughtful editors at *YLPR* (Emma Roberts and Adrianna Duggan in particular), thank you for making this piece infinitely better. You have my utmost admiration.

1. THE POLICE, EVERY BREATH YOU TAKE (A&M Records 1983).

privacy and state action doctrine—establishes that a government purchase is neither a search nor converts service providers or brokers into state actors. As a result, Fourth Amendment doctrine does not regulate a government purchase of sensitive geolocation data. This surprising but inescapable conclusion underscores the urgent need for Congress to pass legislation to regulate private sales and market transactions of these data in the first place—to prevent foreign actors and other companies from getting their hands on our sensitive data, and to revive the foundational promise of the Fourth Amendment.

INTRODUCTION

Weeks after the Supreme Court overturned *Roe v. Wade*, thirteen state legislatures banned and criminalized abortion.[2] Reproductive rights organizations decried the decision as a fundamental erosion of rights, while Republican lawmakers in red states declared the passage of these statutes a moral victory.[3] To third-party data broker SafeGraph, however, *Dobbs* presented a business opportunity.

SafeGraph, like other brokers, purchases users' location data from ordinary apps and from other internet service providers (ISPs).[4] Such data is collected from virtually all applications—prayer apps, mobile games, the weather app, Google, rideshare apps, and more.[5] Brokers, in turn, repackage and sell geolocation data to willing buyers.[6] By aggregating cell service location information (CSLI) and other geolocation data across phone applications and other services, SafeGraph created a data package that

2. Spencer Kimball, *Several U.S. States Immediately Ban Abortion After Supreme Court Overturns Roe v. Wade*, CNBC (Jun. 24, 2022), https://www.cnbc.com/2022/06/24/us-states-immediately-institute-abortion-bans-following-roe-ruling.html [https://perma.cc/7KLF-WCL5].

3. *Reactions To the Supreme Court Overturning* Roe v. Wade, REUTERS (Jun. 26, 2022), https://www.reuters.com/world/us/reactions-us-supreme-court-overturning-roe-v-wade-abortion-landmark-2022-06-24/ [https://perma.cc/NKN4-BK2C].

4. *See* Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022), htttps://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/W9FN-VWAB].

5. Carey Shenkman et al., *Legal Loopholes and Data for Dollars: How Law Enforcement and Intelligence Agencies Are Buying Your Data from Brokers*, CTR. FOR DEMOCRACY & TECH. (Dec. 2021), https://cdt.org/wp-content/uploads/2021/12/2021-12-08-Legal-Loopholes-and-Data-for-Dollars-Report-final.pdf [https://perma.cc/8PX3-GHUS].

6. *Id.*

traced users who visited any of Planned Parenthood's 600 locations across the United States.[7] In the months leading up to the anticipated *Dobbs* decision, purchasers of SafeGraph's "Planned Parenthood" data package could acquire a weeks' worth of location data at a time, which, according to the company, answered questions like "how often people visit, how long they stay, where they came from, where else they go, and more."[8] While SafeGraph "stopped selling information on visits to abortion clinics" in the wake of the leaked *Dobbs* decision,[9] as of August 2022, thirty-two other brokers continued to sell similar data.[10] Among the likely purchasers of these datasets are law enforcement agencies in states that recently banned abortion.[11]

The Fourth Amendment ordinarily requires law enforcement and intelligence agencies to obtain a warrant to conduct surveillance—for example, tracking people's locations and searching their private records.[12] *Katz v. United States* explains that the Fourth Amendment "protects

7. Cox, *Data Broker Is Selling Location Data*, *supra* note 4.

8. *Id.*; *See also Patterns*, SAFEGRAPH, https://docs.safegraph.com/docs/monthly-patterns [https://perma.cc/XP5P-B3BH] (describing the *Patterns* dataset sold by SafeGraph, which is no longer offered, but contained data on users' visits to certain points of interest).

9. Dan Mangan, *Location Data Broker SafeGraph Stops Selling Information on Visits to Abortion Providers*, CNBC (May 4, 2022), https://www.cnbc.com/2022/05/04/data-broker-safegraph-stops-selling-abortion-provider-information.html [https://perma.cc/4NLA-AQ4H] (noting that SafeGraph stopped selling information on visits to abortion clinics "to curtail any potential misuse of its data").

10. Karl Bode, *Rampant Data Broker Sale of Pregnancy Data Gets Fresh Scrutiny Post Roe*, TECHDIRT (Aug. 15, 2022), https://www.techdirt.com/2022/08/15/rampant-data-broker-sale-of-pregnancy-data-gets-fresh-scrutiny-post-roe [https://perma.cc/4Y9A-E9U5]; *see also* Alfred Ng, *Data Brokers Resist Pressure to Stop Collecting Info on Pregnant People*, POLITICO (Aug. 1, 2022) https://www.politico.com/news/2022/08/01/data-information-pregnant-people-00048988 [https://perma.cc/RF5U-33E4] (explaining how data brokers have continued to sell information on pregnant people in the wake of the *Dobbs* decision and have resisted lawmakers' pressure to stop).

11. *Post-Roe, Civil Society Calls on Data Brokers to Do No Harm*, ACCESSNOW (Jan. 26, 2023), https://www.accessnow.org/press-release/post-roe-data-brokers [https://perma.cc/8W82-D5GB].

12. United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 324 (1972).

individual privacy against certain kinds of governmental intrusion."[13] Under the *Katz* privacy test, a search occurs when "a person ha[s] exhibited an actual (subjective) expectation of privacy and . . . the expectation be one that society is prepared to recognize as 'reasonable.'"[14] Thus, when the government invades a user's reasonable expectation of privacy, it must obtain a warrant.[15]

Historically, this provision of the Bill of Rights has struggled to keep pace with the novel privacy issues that attend evolving surveillance methods.[16] In 2018, however, the Supreme Court ruled that users have a reasonable expectation of privacy in historic CSLI data.[17] Since cellphone use is "almost a 'feature of human anatomy,'" historical location data presents a near infallible record of every location a user has frequented.[18] People do not relinquish their privacy expectations in these data merely because their phones transmit their real-time location to a third party (i.e.,

13. 389 U.S. 347, 350 (1967).

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

15. This is relevant doctrinal inquiry for data purchases, but under current doctrine, searches can also occur in circumstances involving trespass. When the government "physically occupie[s] private property for the purpose of obtaining information," a search occurs. United States v. Jones, 565 U.S. 400, 404-05 (2012). "[S]uch a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted." *Id.* Accordingly, this branch of Fourth Amendment doctrine is "tied to common-law trespass." *Id.* at 405. Such a physical intrusion occurs when the government enters onto a person's property, or even when the government places a tracking device on a suspect's car. *Id.* at 404–05. Obviously, though, no physical intrusion transpires when an agency purchases records from brokers that users may not even know exist.

16. *See* Robert S. Litt, *The Fourth Amendment in the Information Age*, 126 YALE L.J.F. (Apr. 27, 2016), https://www.yalelawjournal.org/forum/fourth-amendment-information-age [https://perma.cc/FFG3-CQK8] ("To badly mangle Marx, a specter is haunting Fourth Amendment law—the specter of technological change. In a number of recent cases, in a number of different contexts, courts have questioned whether existing Fourth Amendment doctrine, developed in an analog age, is able to deal effectively with digital technologies.").

17. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) ("A person does not surrender all Fourth Amendment protection by venturing into the public sphere . . . . Allowing government access to cell-site records contravenes that expectation [of privacy].").

18. *Id.* at 2218 (quoting Riley v. California, 573 U.S. 373, 385 (2014)).

the internet service providers (ISPs)): phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[19] Compelling ISPs to hand over CSLI data, then, required the government to obtain a warrant. This denoted a landmark moment for privacy in the digital age: for the first time, users had Fourth Amendment rights in records they "likely [did] not even know exist[ed]."[20]

Rather than obtain a warrant to compel private actors to hand over this sensitive geolocation information, however, the government now simply *purchases* mass records from third-party brokers—without a warrant. The Department of Homeland Security (DHS) alone has spent millions of dollars buying CSLI data from two data brokers, Venntel and Babel Street, since 2017.[21] The Federal Bureau of Investigation (FBI)[22] and the Drug Enforcement Agency (DEA)[23] have purchased services and data from Venntel, a broker whose parent company claims to have access to location

19. *Id.* at 2220 (quoting *Riley*, 573 U.S. at 385); *see also id.* (quoting Smith v. Maryland, 442 U.S. 735,735 (1979)) ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.").

20. Orin S. Kerr, *Buying Data and the Fourth Amendment*, *in* HOOVER INST., AEGIS PAPER SERIES 1 (2021).

21. Nihal Krishan, *DHS Buying Personal Data from Govt Contractors Pushes Congress to Pass Legislation Curtailing 3rd Party Data Brokers*, FEDSCOOP (July 22, 2022), https://fedscoop.com/dhs-buying-personal-data-from-govt-contractors-pushes-congress-to-pass-legislation-curtailing-3rd-party-data-brokers [https://perma.cc/RZ9N-EASQ]; *ACLU v. Department of Homeland Security (Commercial Location Data FOIA)*, ACLU (July 18, 2022), https://www.aclu.org/cases/aclu-v-department-homeland-security-commercial-location-data-foia [https://perma.cc/K3TB-GZWS] (compiling materials, including DHS contracts with Venntel and Babel Street, that were released under an ACLU FOIA request).

22. *FBI Records: Contract with Venntel,* FBI, https://vault.fbi.gov/contract-with-venntel/contract-with-venntel-part-01-of-01/view [https://perma.cc/2U2E-BHNC].

23. Joseph Cox, *The DEA Abruptly Cut Off Its App Location Data Contract*, VICE (Dec. 7, 2022), https://www.vice.com/en/article/z3v3yy/dea-venntel-location-data [https://perma.cc/LA2R-WMBU].

data on over 150 million devices.[24] The Defense Intelligence Agency (DIA) has also confirmed that it avails itself of third-party brokers' data.[25] Even local police have purchased sensitive location data from brokers to support law enforcement investigations.[26]

Warrantless purchases do not violate existing statutory frameworks,[27] and courts have yet to pronounce on the constitutionality of the practice. While government agencies "do[] not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes,"[28] numerous op-eds suggest the agency "interpretation is certainly vulnerable to legal challenge."[29] But

24. *Frequently Asked Questions,* GRAVYANALYTICS (2023), https://gravyanalytics.com/frequently-asked-questions [https://perma.cc/548X-KPMF]. GravyAnalytics, Venntel's parent company, provides Venntel with "much of its data." *See* Bennett Cyphers, *How the Federal Government Buys Our Cell Phone Location Data*, ELEC. FRONTIER FOUND. (June 13, 2022), https://www.eff.org/deeplinks/2022/06/how-federal-government-buys-our-cell-phone-location-data [https://perma.cc/36VC-JCQ9].

25. Cyphers, *supra* note 24.

26. Press Release, Elec. Frontier Found., Data Broker Helps Police See Everywhere You've Been with the Click of a Mouse: EFF Investigation (Sep. 1, 2022), https://www.eff.org/press/releases/data-broker-helps-police-see-everywhere-youve-been-click-mouse-eff-investigation [https://perma.cc/ZK8J-B5C7].

27. The 1986 Electronic Communications Privacy Act (ECPA) was specifically passed to "limit the government's ability to access digital communications, or information about such communications, without adhering to certain legal standards." The ECPA only applies to certain categories of computing and communication service providers, but it "does not reference modern data brokers, which did not exist in the 1980s." Brokers thus fall outside the scope of ECPA regulation. *See* Shenkman et al., *supra* note 5, at 15.

28. Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 25, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [https://perma.cc/9J6Q-ZEXD].

29. Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, WASH. POST (Apr. 26, 2021, 6:00 AM EDT), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases [https://perma.cc/W3NY-Q2BG]. *See also* Matthew Tokson, *Government Purchases of Sensitive Private Data*, DORF ON L. (Mar. 29, 2021), https://www.dorfonlaw.org/2021/03/government-purchases-of-sensitive.html [https://perma.cc/CVT2-HMX3].

these short commentaries forego in-depth doctrinal analysis, and "it could be years before the courts resolve the issue."[30] Instead, a group of twenty senators have introduced the Fourth Amendment Is Not For Sale Act (FAINFSA) to preemptively close this *potential* loophole in Fourth Amendment doctrine.[31] This law would ban government agencies from obtaining location information, the contents of communications, and other kinds of sensitive data "in exchange for anything of value."[32]

Over two years have elapsed since legislators first proposed the law.[33] As the House has voted to reintroduce FAINFSA, the time is ripe for a full examination of whether an agency purchase of sensitive data from third-party brokers requires a warrant under the Constitution and whether FAINFSA is the best way to fill any constitutional gaps. This Note hence examines whether the Fourth Amendment regulates law enforcement and intelligence agencies' purchases of sensitive location data.[34]

To accomplish this, the Note employs a two-part inquiry. Axiomatically, the Fourth Amendment only protects against "unreasonable searches" of people's private records by the *government*.[35] Therefore, it first asks (I)

30. Goitein, *supra* note 29.

31. *Id.*

32. Fourth Amendment Is Not For Sale Act, S. 1265 177th Cong. § 2 (2021).

33. *Id.*

34. Note that there are special "administrative searches" that apply to searches conducted for other purposes. The warrant requirement does not ordinarily apply to these administrative searches. *See* New York v. Burger, 482 U.S. 691 (1987) (upholding a New York statute authorizing warrantless inspections of junkyards and other "closely regulated" industries). This Note instead focuses on purchases by law enforcement and intelligence agencies which represents a vast majority of purchases in the market.

35. Burdeau v. McDowell, 256 U.S. 465, 475 (1921). The cornerstone constitutional provision was a reaction to general warrants. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 785-86 (1994); 2 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES 609 (2d. ed. photo. reprt. 2005) (1851). In the colonial period, general warrants allowed agents of the Crown to search people, their homes, and their personal documents arbitrarily and invasively. *See* WILLIAM J. CUDDIHY, THE FOURTH AMENDMENT: ORIGINS AND ORIGINAL MEANING, 602-1791 at 232-244 (2009); *see also* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 42-49 (1937) (describing the use of general warrants in seditious libel cases in England from 1695-1760 and successful challenges to them post-1760); Walter B. Hamlin, *The Bill of*

whether a government purchase of data is "state action." Then, it determines (II) whether users have a reasonable expectation of privacy in commercially available data (i.e., the *Katz* privacy test). For the Fourth Amendment to apply, *both* (I) and (II) must be answered in the affirmative.

This Note—the first comprehensive examination of government purchases under the state action doctrine[36]—proceeds in three parts. Part I addresses the first prong of the inquiry: it demonstrates that an agency purchase of data is not "state action" in the constitutional sense, and thus, the Fourth Amendment does not apply to these purchases. This Part then establishes that an open-market government purchase of user data does not convert either a service provider or data broker into a "state actor." As a result, the Fourth Amendment does *not* prohibit a warrantless purchase of sensitive records.

Part II concerns the second prong of the two-part inquiry: it shows that users have a reasonable expectation of privacy in the location records sold by data brokers. Agency lawyers have suggested that users cannot have privacy expectations in commercially available data.[37] Yet this Note—the

---

Rights or the First Ten Amendments to the United States Constitution, 68 COM. L.J. 233, 235 (1963) (describing colonial judges, notably in Massachusetts, granting general warrants for customs officers to search for contraband at "all times and all occasions"); Tracey Maclin, *The Complexity of the Fourth Amendment: A Historical Review*, 77 B.U. L. REV. 925, 939-40 (1997) ("[M]ost search warrants issued during the colonial period authorized general searches."). As it was intended as protection against the emergence of an Orwellian police state, the Fourth Amendment does not protect against searches conducted by strictly private actors. See discussion *infra* Section III.A.

36. The existing scholarship—composed of two student notes, one blog post, and one Brookings essay—assumes that whether an agency may purchase these intrusive datasets without a warrant turns solely on whether users have a reasonable expectation of privacy. They either do not address the state action problem or they assume the data brokers are state actors. *See* Jillian Chambers, Note, *Carpenter, the Fourth Amendment, and Third-Party Workarounds*, 53 CONN. L. REV. 183 (2021); Dori H. Rahbar, Note, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates* Carpenter *and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713 (2022); Tokson, *supra* note 29; Kerr, *supra* note 20. Orin Kerr even expresses that "it is unclear how the state action doctrine applies to sales of records" and instead "put[s] those potentially tricky issues aside." *Id.* at 11 n.4.

37. Tokson, *supra* note 29; *see also* Savage, *supra* note 28 (noting that DIA does not believe it needs a warrant to purchase location data, though whether that

first in-depth assessment of this intuitive argument—advances that users *do* retain privacy rights in commercially available geolocation data. The fact that users agree to data-sharing provisions in Terms of Service Agreements does not undermine this conclusion, nor could ISPs or data brokers consent to a search on users' behalf. But-for the state action problem, then, users would be protected from warrantless purchases of data.

In Part III, I demonstrate that this awkward result is in tension with the underlying purpose of the Fourth Amendment. Though not forged as a bulwark for privacy, this cornerstone constitutional protection was (partially) intended to shield people's private lives—their political beliefs, religious associations, and personal activities—from government scrutiny.[38] By keeping personal lives invisible to prying government eyes, the Fourth Amendment hides people's unorthodoxy and private dissent—the very things that could subject them to unjust persecution. Yet geolocation data can reveal precisely these same intimate aspects of our private lives: our faith,[39] political associations and beliefs,[40] sexual orientation,[41] immigration status,[42] and much more. There ought to be *some* protections against purchases of these location data, even if this protection does not fit within the confines of the Fourth Amendment.

---

belief rests on the idea that users cannot have a privacy expectation in that data is unclear).

38. See discussion *infra* Section III.A.

39. *See* Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE (Nov. 16, 2020, 3:35 PM), https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/BWZ4-8PSZ].

40. *See* Sidney Fussell, *The Most Important Things to Know About Apps That Track Your Location*, TIME (Sept. 1, 2022, 2:13 PM EDT), https://time.com/6209991/apps-collecting-personal-data [https://perma.cc/9NUW-H35U]; Jennifer Valentino-DeVries et al., *Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret*, N.Y. TIMES (Dec. 10, 2018), www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html [https://perma.cc/7GVP-3LAV].

41. Heather Kelly, *A Priest's Phone Location Data Outed His Private Life. It Could Happen To Anyone*, WASH. POST (July 22, 2021), https:// www.washingtonpost.com/technology/2021/07/22/data-phones-leaks-church/ [https://perma.cc/K5JP-XZBA].

42. *See* Cristiano Lima, *ICE's Use of Data Brokers To 'Go Around' Sanctuary Laws Under Fire*, WASH. POST (July 27, 2022, 8:52 AM EDT), https://www.washingtonpost.com/politics/2022/07/27/ices-use-data-brokers-go-around-sanctuary-laws-under-fire [https://perma.cc/9D7Q-TLCV].

Blanketly preventing *only* U.S. government agencies from purchasing these data (for example, through FAINFSA), would be misguided, however. Under FAINFSA, data brokers may not sell sensitive information to the U.S. government without a warrant, but they would still be free to sell to hostile foreign actors and governments without constraint. This creates a serious foreign intelligence threat. Instead, Congress must step in and pass privacy legislation to address this issue at its source by regulating transactions of sensitive data in the first place.

I. SHORT-CIRCUITING THE WARRANT REQUIREMENT: THE STATE ACTION PROBLEM

The Fourth Amendment only protects people against unreasonable searches by the *government*, not from those conducted by purely private parties.[43] Thus, for the Fourth Amendment to require a warrant to purchase commercial geolocation data, the act of purchasing data itself must be considered a "government search" or "state action." Even if users have a reasonable expectation of privacy in their commercial geolocation records under *Carpenter*, the government need not obtain a warrant if a purchase is not "state action."

Courts have never directly addressed the question of whether a purchase can constitute a search in itself, and indeed, existing commentary also fails to address the significance of the state action question. Dori Rahbar, Matthew Tokson, and Jillian Chambers claim that a purchase of data from brokers is a search because users have a reasonable expectation of privacy in these records, but they do not evaluate whether the purchase is a "state action."[44] This reflects a view of the Fourth Amendment as agnostic to the form of acquisition. But even Orin Kerr, who defends the constitutionality of the practice, expresses that "it is unclear how the state action doctrine applies to sales of records."[45]

This section therefore addresses the first prong of the two-part inquiry: the state action problem. Two crucial yet underexplored doctrines point to the regrettable but inescapable conclusion that a purchase of data packages cannot constitute a search. First, under the "recurrent access" doctrine, a

43. Burdeau v. McDowell, 256 U.S. 465, 475 (1921). *See also* United States v. Jacobsen, 466 U.S. 109, 115 (1984) ("Whether those invasions were . . . reasonable or unreasonable, they did not violate the Fourth Amendment because of their private character.").

44. *See supra* note 36, and accompanying text.

45. Kerr, *supra* note 20, at 11 n.4.

government acquisition of private material is *not* a search if (i) the material was already the subject of a private search, (ii) the private actor who conducted the private search voluntarily transferred that material to the government, and (iii) the government's acquisition and use of the material did not extend past the scope of the private search.[46] A government purchase of records satisfies these criteria required by the recurrent access doctrine. Second, under other provisions of the Constitution, the government does not undertake any "state action" when operating as a mere market participant. A purchase thus cannot qualify as a government search. Agency purchases of sensitive data from private third-party corporations do not qualify as state action under either of these tests.

After asserting that a purchase is not state action and therefore not a search, this Part contemplates whether an agency purchase transforms either the ISP or data broker into a state actor. This Note concludes it does not and establishes that the Constitution permits warrantless agency purchases of sensitive, invasive data, regardless of whether users have a reasonable expectation of privacy in the commercial records.

A. Is a Government Purchase a Search? The "Recurrent Access" and "Market Participant" Doctrine

When a private actor searches another person (and so, violates their reasonable expectation of privacy), the government itself violates the Fourth Amendment insofar as it *compels* (without a warrant or subpoena) the private searcher to hand over the information obtained from the search.[47]

However, when a private party invades a person's reasonable expectation of privacy and *voluntarily* hands over that information to the government, the government's acquisition is not itself a search.[48] In *United*

46. *Jacobsen*, 466 U.S. at 115-18.

47. *See* Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018) ("Before compelling a wireless carrier to turn over a subscriber's CSLI, the government's obligation is a familiar one—get a warrant."); *Burdeau*, 256 U.S. at 476 (explaining that if a third party wrongfully obtained incriminating documents, and the government "had no part in wrongfully obtaining them," there is "no reason why a subpoena might not issue for the production of the papers as evidence").

48. Walter v. United States, 447 U.S. 649, 656 (1980) ("[T]here [was] nothing wrongful about the Government's acquisition of [private] packages or its

States v. Jacobsen, the Supreme Court held that "additional invasions of respondents' privacy by the government agent must be tested by the degree to which they exceeded the scope of the [initial] private search."[49] Only if the government's subsequent actions reveal more than what the private search already revealed can there be a government search.

The opinions in *Walter v. United States* illuminate how the court arrived at this reasoning. In *Walter*, a private party opened a clearly mistakenly delivered package, revealing rolls of contraband motion picture material.[50] The initial opening of this package constituted a "limited private search" which violated the intended consignee's reasonable expectation of privacy.[51] The private party then *voluntarily* turned the carton over to the FBI, which viewed the films.[52] *Walter* had no majority opinion, but four years later in *Jacobsen*, the Court characterized the separate *Walter* opinions. The *Jacobsen* Court noted that "a majority [of justices in *Walter*] agree[d] on the appropriate analysis of a governmental search that follows on the heels of a private one": a government search only occurs insofar as the government's actions reveal more than what the private search exposed.[53] Thus, even if the initial material carries a reasonable expectation of privacy, a government acquisition of information already obtained by a private party is not necessarily a search.

The Supreme Court's decision in *Jacobsen* consolidated the disparate *Walter* opinions to clarify this principle. The *Jacobsen* Court explained that a government examination of private material on the heels of a private search must be "tested by the degree to which they exceeded the scope of the private search,"[54] the standard adopted by a majority of justices in *Walter*.[55] In *Jacobsen*, the Court therefore held:

---

examination of their contents to the extent that they had already been examined by third parties.").

49. *Jacobsen*, 466 U.S. at 115.

50. *Walter*, 447 U.S. at 651-52.

51. *Id.* at 656.

52. *Id.* at 652.

53. *Id.*

54. *Jacobsen*, 466 U.S. at 115.

55. Two Justices in *Walter* asserted that if "the results of [a] private search are in plain view when materials are turned over to the Government," the existence of the initial private search "may justify the Government's reexamination of the materials." However, the "Government may not exceed the scope of the

> The Fourth Amendment is implicated only if the authorities use information with respect to which the expectation of privacy has not already been frustrated. In such a case the authorities have not relied on what is in effect a private search, and therefore presumptively violate the Fourth Amendment if they act without a warrant.[56]

By contrast, when the government relies strictly on a private search, and the government did not force the private party to hand over the searched material, no warrant is needed. Government authorities, therefore, do not need to obtain a separate warrant where (i) the search is confined to the scope of the private search, and (ii) the material obtained from the private search is handed over voluntarily to the government.

Applying this framework, the *Jacobsen* Court concluded that a government agent did not need a warrant to search a package previously examined by a private Federal Express employee. After all, the government's examination "enabled the agent to learn nothing that had not previously been learned during the private search."[57] The "agent's viewing of what a private party had freely made available for [the government's] inspection did not violate the Fourth Amendment."[58]

Lower court rulings on recurrent access to prior private searches are consistent with *Jacobsen* and *Walter*. For example, in *United States v. Lichtenberger*, a suspect's girlfriend opened the suspect's laptop, and "then showed [an] officer a *sample* of what she had found."[59] The Sixth Circuit noted that "this fact pattern was analogous to the critical elements of

---

private search unless it has the right to make an independent search." *Id.* at 116 (quoting *Walter*, 447 U.S. at 657 (opinions of Stevens, J., joined by Stewart, J.). According to *Jacobsen*, the four Justices in the *Walter* plurality "were also of the view that the legality of the governmental search must be tested by the scope of the antecedent private search"––they simply disagreed with the other Justices' characterization of the factual scope of the private search. *Id.* at 116 (quoting *Walter*, 447 U.S. at 657 (opinions of Stevens, J., joined by Stewart, J.). After all, the *Walter* plurality clarified that had the private party in *Walter* "so fully ascertained the nature of the films before contacting the authorities," the "FBI's subsequent viewing of the movies on a projector [would] not 'change the nature of the search' and [would] not [constitute] an additional search subject to the warrant requirement." *Jacobsen*, 466 U.S. at 116.

56. *Id.* at 117-18.

57. *Jacobsen*, 466 U.S. at 120.

58. *Jacobsen*, 466 U.S. at 119.

59. 786 F.3d 478, 484 (6th Cir. 2015) (emphasis added).

Jacobsen—a private search followed closely by a governmental search."[60] But unlike *Walter*, the officer's subsequent search involved a complete review of the laptop's files, even though the girlfriend had revealed only a "sample of what she had found."[61] Had the officer's search not "exceeded [the scope] of [the girlfriend's] private search," the court would have held no government search occurred—even though the original material was protected by a reasonable expectation of privacy.[62] Indeed, even when people have a reasonable expectation of privacy in documents or other materials within the scope of a private search, the government still need not obtain a warrant to search these materials provided the search meets the requirements of the recurrent access doctrine. The Ninth Circuit, Sixth Circuit, and Eighth Circuit have made this point clear.[63]

A government purchase of data is "analogous to the critical elements of *Jacobsen*—a private search followed closely by a governmental search."[64] Thus, whether a government purchase is itself a "search" turns on (i) whether the government's actions extend past the scope of the data broker's private search, and (ii) whether the private party transferred the material to the government voluntarily.

---

60. *Id*.

61. *Id*.

62. *Id*. at 485.

63. This suggests that *Carpenter v. United States*, discussed subsequently, does not change the doctrinal outcome, for it has no bearing on the recurrent access doctrine. Kleiser v. Chavez, 55 F.4th 782, 783 (9th Cir. 2022) ("Mr. Electric contends that *Carpenter* . . . extinguish[es] the applicability of the private search exception to the Fourth Amendment to location information. This argument overreads the case law. [While] *Carpenter* held that the third-party doctrine does not apply as an exception to the Fourth Amendment's warrant requirement when the government seeks cell site location information . . . . The private search exception is an altogether separate exception to the Fourth Amendment."). In this case, a disgruntled private employee disclosed CSLI data to the government, and the government did not need a warrant to use the information. United States v. Miller, 982 F.3d 412, 431 (6th Cir. 2020) ("*Carpenter* asked only whether the government engaged in a 'search' when it compelled a carrier to search its records for certain information that the government demanded," but "did not cite *Jacobsen*, let alone address its private-search doctrine."). United States v. Ringland, 966 F.3d 731, 737 (8th Cir. 2020) (Finding *Carpenter* did not apply in a case concerning the recurrent access doctrine.).

64. *Lichtenberger*, 786 F.3d at 484.

Addressing the first factor, when the government purchases a dataset, it conforms to the scope of the private search. Private parties thoroughly examine and process their data packages before the records change hands. The government therefore does not extend past the boundaries of the original search.

Some may reasonably suggest that a government's acquisition of these same records *could* reveal more than the private search alone, even if the agency processes and examines the dataset no more thoroughly than the data brokers. This reflects the "mosaic theory" of the Fourth Amendment: while a single datapoint might reveal little in isolation, when put in conversation with other data, they reveal much more invasive and intimate information about a person—and so, can constitute a search.[65] In this case, the government might have access to such additional datasets that, when paired with the new acquisition, reveal more about their targets of surveillance.

Although the Supreme Court has debatably adopted this approach in some contexts,[66] *Jacobson* rejects this argument as applied to the types of aggregate purchases of private data discussed here. *Jacobsen* specifically contemplated that the FBI might have information about a particular suspect that, when put together with the reexamination of a private search, unveils even more about the private party than the initial search.[67] Yet that was not enough to suggest there was an "additional search" creating a

65. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 320 (2012) ("[T]he mosaic theory asks whether a series of acts that are not searches in isolation amount to a search when considered as a group.").

66. *See Carpenter*, 138 S. Ct. at 2217-18 (Stressing that historical CSLI data *in aggregate* allows for "near perfect surveillance."); Taylor Wilson, Note, *The Mosaic Theory's Two Steps: Surveying Carpenter in the Lower Courts*, 99 TEX. L. REV. ONLINE, 156 ("In *Carpenter*, the Court seemed to accept the mosaic theory by considering the data presented as a group."); Robert Fairbanks, Note, *Masterpiece or Mess: The Mosaic Theory of the Fourth Amendment Post-*Carpenter, 26 BERK. J. CRIM. L. 71, 73 (2022) ("In *Carpenter v. United States*, the Supreme Court . . . potentially adopted what has been called the mosaic theory of the Fourth Amendment"). *But see Carpenter*, 138 S. Ct. at 2217 n.3 ("[W]e need not decide whether there is a limited period for which the Government may obtain an individual's historical CSLI free from Fourth Amendment scrutiny, and if so, how long that period might be.").

67. *Jacobsen,* 466 U.S. at 119 (Finding it "hardly infringed respondents' privacy for the agents to reexamine the contents" even where the government had independent testimony on the respondent and the contents of the package in question).

separate invasion of privacy. Purchases of data thus do not transgress the scope of the initial private search, because the recurrent access doctrine expressly set aside mosaic theory-based considerations.

The remaining question, then, is whether an open-market transaction with the government counts as a voluntary transfer of a private search to the government.

Longstanding Fourth Amendment doctrine suggests that open-market transactions are presumptively voluntary. In the defining case *Maryland v. Macon*, an undercover official purchased obscene material from a willing seller. Crucially, that meant the vendor was not aware he was selling to law enforcement, and thus, sold the material *without* bending to any government pressure. Even though the government official sought to purchase the material, the Court held that the seller transferred it voluntarily. Any Fourth Amendment rights thus went away with the voluntary sale.[68] Since then, the Court has routinely made clear that even where the government's identity is known, open market sales are presumptively voluntary on the private party's behalf.[69]

There is no reason to doubt that brokers sell data packages to the government voluntarily. The market is estimated to be worth several billions.[70] Individual data brokers stand to profit enormously from selling user records, whether to advertisers or to the government.[71] And as discussed later in this section, the mere fact that the private actors stand to profit enormously is not enough to render a purchase involuntary.[72] This distinguishes situations where a private corporation is compelled by law enforcement to hand over data from a voluntary sale.[73]

68. Maryland v. Macon, 472 U.S. 463 (1985).

69. *See, e.g.*, United States v. Testan, 424 U.S. 392 (1976) (when respondent entered into an employment agreement with the United States, that transactional decision was voluntary, rather than induced or compelled); Taylor v. Taintor, 83 U.S. 366, 372 (1872) (transaction with government with respect to a bounty hunting contract was entered into voluntarily, not an inducement). See also discussion on inducement, *infra* Section I.B.2.

70. David Lazarus, *Shadowy Data Brokers Make the Most of their Invisibility Cloak*, L.A. TIMES (Nov. 5, 2019), https://www.latimes.com/business/story/2019-11-05/column-data-brokers [https://perma.cc/SG3W-8N6P].

71. *Id*.

72. *See* discussion *infra* Section III.B.2.

73. This is what occurred in *Carpenter*, 138 S. Ct. 2206: the government compelled an ISP to hand over detailed CSLI data without a warrant. This constitutes state action.

Furthermore, under other provisions of the Constitution, not all of the government's actions are regulated equally. When the government acts as a mere market participant, but does not exercise "coercive power," its actions do not count as "state action."[74] For example, in *San Francisco Arts and Athletics v. United States Olympic Committee*, the U.S. Olympic Committee's "choice of how to enforce its exclusive [trademark] right to use the word 'Olympic' *simply* [was] *not a governmental decision*."[75] In *Brentwood Academy v. Tennessee Secondary School Athletic Association*, the Court similarly held that certain decisions taken by a school association as a market participant—such as the sale of advertising—did not constitute state action.[76] An agency buyer of data is definitionally a mere market participant, especially since advertisers buy data packages too. As a result, a government purchase is not state action, and so, cannot constitute a government search regulated by the Fourth Amendment.

However, just because the government's purchase of the data itself does not constitute state action does not end the inquiry: it remains possible that the prospect of a government purchase transformed either the service provider or the data broker into arms of the government.

B. Do Government Purchases Convert Service Providers or Data Brokers into State Actors?

Even if the Fourth Amendment does not ordinarily regulate private actors, it does prohibit warrantless searches by private parties acting as mere instruments or agents of the government.[77] Finding that the government purchase converted either the ISP or brokers into state actors requires serious contorting of the doctrine, however. As a result, this Note suggests a government purchase does not implicate state action at all.

The touchstone of state action analysis is in the government's level of "entwinement" with a private party's actions. Here, the government buyer is uninvolved in the ISP's initial collection of records and is not party to the sale of those records to the data brokers. Nor can it even be said that a

74. San Francisco Arts & Athletics, Inc. v. U.S. Olympic Comm., 483 U.S. 522, 547, (1987).

75. *Id.* at 547 (emphasis added).

76. 531 U.S. 288 (2001).

77. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602 (1989); U.S. v. Jacobsen, 466 U.S. 109, 113-14 (1984); Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

broker's sale of user data created state action, for open-market transactions do not ordinarily convert sellers into arms of the government.

State action doctrine further recognizes private actors as subject to the Bill of Rights when the government has *induced* a private party to do what it is constitutionally forbidden to do itself.[78] But even if the government offers huge monetary reward for access to the data packages brokers sell, economic incentive, no matter how large the potential windfall, does not ordinarily count as inducement for state action purposes.

Finally, private actors can be held accountable under the Fourth Amendment if they fulfill a public function traditionally reserved to the state. This exception is narrow, however, and its numerous conditions would not apply to the case of a data purchase.

This Note thus argues that an agency purchase converts neither the ISP's initial collection nor the subsequent sales of data into compelled state action. No state action is implicated by a government purchase of data, and so, these transactions fall outside the scope of constitutional scrutiny.

1. Is the ISP's Initial Collection of Data "State Action"? What About Its Sale of Data to the Brokers?

Matthew Tokson cites the recent District Court decision in *Cooper v. Hutcheson* to gesture at the idea that a government purchase converts service providers into state actors for Fourth Amendment purposes.[79] In that case, Securus, a private company, sold a product designed to track suspect locations in criminal investigations. Securus "argue[d] that it [could] not be liable under § 1983 because it is not a state actor."[80]

The District Court recounted that the "Supreme Court has recognized several circumstances in which a private party may also be characterized as a state actor."[81] These include "where a private actor is a 'willful participant in joint activity with the State or its agents,'" or "where there is 'pervasive entwinement' between the private entity and the state."[82] Tokson thus concludes that "[b]ecause Securus was a willful participant in joint surveillance activity with the government, it could be considered a state

78. Blum v. Yaretsky, 457 U.S. 991, 1004 (1982).

79. Tokson, *supra* note 29.

80. Cooper v. Hutcheson, 472 F. Supp. 3d 509, 513 (E.D. Mo. 2020).

81. *Id*.

82. *Id*.

actor for Fourth Amendment purposes."[83] Based on this case, Tokson advances that service providers could similarly be considered a "willful participant" in government surveillance.[84]

Tokson overstates *Cooper*'s applicability to the question at hand. *Cooper* resolved a Motion to Dismiss, in which the District Court needed not conclude there was willful participation in a public function, but instead, merely a plausible inference of such.[85] More importantly, in *Cooper*, the Sheriff contracted to use Securus' location-tracking service *to collect information himself.*[86] The Sheriff did *not* purchase data collected independently by Securus.

When the government purchases a dataset from a broker, an ISP is neither a "willful participant in joint activity with the State or its agents" nor "pervasive[ly] entwine[d]" with the government.[87] Private actors are "willful participants in joint activity" with the government when they directly collaborate with law enforcement and take direction from the government. This occurs, for example, when private parties work with and take direction from state officials to seize property.[88] Meanwhile, courts

83. Tokson, *supra* note 29.

84. *Id.* ("[T]he Sheriff's use of a vendor didn't allow him to circumvent the Fourth Amendment. At least where vendors cater to law enforcement customers and provide them with services designed for tracking individuals, government purchases of location data are likely to require a search warrant.").

85. *Cooper*, 472 F. Supp. 3d at 513 ("[T]he Court concludes that, at this stage of the proceeding, Plaintiffs have alleged sufficient facts from which the Court could reasonably conclude that Securus was a "willful participant in joint activity with the State or its agents."). To survive a motion to dismiss under Rule 12(b)(6), a complaint must plead "enough facts to state a claim to relief that is plausible on its face." *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). A claim has "facial plausibility when the plaintiff pleads factual content that allows the Court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009).

86. *Id*. at 512-513 (internal references omitted) ("Defendant Cory Hutcheson was the Sheriff for Mississippi County and had access to the Securus LBS program and used it to conduct unauthorized searches on Plaintiffs and others . . . . Put simply, the Mississippi County Sheriff's Department could not conduct LBS tracking without Securus and Securus—which asserts that its users are 'exclusively law enforcement personnel'—sells a product designed to be used in tracking individuals for criminal investigation. Securus is a willing participant in the joint activity of conducting LBS searches.").

87. *Id.* at 513.

88. Lugar v. Edmondson Oil Co., 457 U.S. 922, 942 (1982).

only find "pervasive entwinement" when government actors are themselves integrated into the private party's internal structure, or a statutory scheme compels private parties to work with the government.[89] Under the Fourth Amendment, this requires direct and heavy-handed involvement from the authorities during the *initial search*—even if the material ends up in government hands. In the common carrier context, government regulations require airlines to hand over seized illegal material to the Transportation Security Administration or FBI; yet, because the search that leads to the (government) seizure does not involve any government agents, the initial search is wholly private.[90] In short, under both doctrines, *direct government involvement* in the initial search is required to render a private search a government search.

Government purchasers of data are not at all involved in the initial collection of user data by ISPs. Agencies do not direct ISPs to collect people's data nor compel them to sell data to the brokers. All circuits agree that more than "mere knowledge and passive acquiescence by the Government" is required to render the private actor an arm of the government.[91] But the government does not even have "mere knowledge" in this case. Government actors may know whose data was collected *ex post*, but at the time of collection, they do not specifically know who the ISPs were tracking. Similarly, the government is not involved in the transaction between ISPs and data brokers, nor does it specifically know whose geolocation data the ISP sells to which brokers. Thus, service providers are neither "pervasive[ly] entwine[d]" nor "willful participants in joint activity" with the government. The initial collection and sale of data by ISPs therefore do not constitute state action under these formulations.

89. Brentwood Acad. v. Tennessee Secondary Sch. Athletic Ass'n, 531 U.S. 288, 291 (2001) ("We hold that the association's regulatory activity may and should be treated as state action owing to the pervasive entwinement of state school officials in the structure of the association.").

90. *See, e.g.*, U.S. v. Sherwin, 539 F.2d 1, 6 (9th Cir. 1976) ("In light of the above, we reach the unmistakable conclusion that the truck terminal manager in this case was not acting as an instrument of the government. There was no official involvement until after the terminal manager had completed his search and called the FBI."); United States v. Kelly, 529 F.2d 1365, 1368, 1371, 1378 (8th Cir. 1976) (same). Even if, somehow, the sale of records was involuntary, the Common Carriers cases would suggest the initial search by the ISP was not.

91. *See, e.g.*, U.S. v. Jarrett, 338 F.3d 339, 345 (4th Cir. 2003); U.S. v. Ellyson, 326 F.3d 522, 527-38 (4th Cir. 2003); U.S. v. Smythe, 84 F.3d 1240, 1242-43 (10th Cir. 1996); U.S. v. Koenig, 856 F.2d 843, 850 (7th Cir. 1988).

Notably, however, state action can be found outside these two circumstances. Whether a private company was acting as an arm of the government is a case-by-case determination, viewed in the totality of the facts, and turns on the degree of government involvement in the private party's activities.[92] Courts use three factors (the "*Walter* factors") to determine if sufficient government involvement exists to convert a private search into government action: (i) the advice, direction, and level of participation given by the government; (ii) whether the motive of the private actor was to assist law enforcement; and (iii) compensation or other benefits the private actor receives from the government.[93] Ultimately, these questions are used to determine if the private actor, in collecting or transferring information, was bending to the will of the government.

Even under these factors, a government purchase alone cannot transform the ISP's initial collection (or its decision to sell user data to brokers) into compelled government action. First, as already established, government purchasers do not furnish advice, give direction, or participate in the initial collection of data by the ISPs. They furthermore are uninvolved in the initial sale of data from ISPs to the brokers. Without contemporaneous knowledge of whose information the ISP collects and sells, the government logically cannot instruct the ISPs on who to surveil.

Second, the ISPs' purpose in collecting and selling geolocation data to brokers is driven by their ability to profit from selling user data, regardless of the buyer. The motive of the ISP, then, is to further its own ends—profit—and not to assist law enforcement. This factor, too, militates against finding state action.[94] Third, the ISP does not receive compensation or other benefits from the government; they sell to the brokers or to advertisers directly.

The *Walter* factors, then, discourage a finding of state action. In no way does a government purchase of records from a data broker convert the initial collection into state action: the ISP does not bend to the will of the government because of the indirect possibility of a purchase from a data broker. Ultimately, the government does not direct initial collection nor influence ISPs to sell user data to brokers. Nor is the prospect of a

92. Skinner v. Railway Labor Executives' Ass'n, 489 U.S. 602, 614-15 (1989).

93. Walter v. United States, 447 U.S. 649, 662 (1980).

94. *See, e.g.*, United States v. Soderstrand, 412 F.3d 1146, 1153 (10th Cir. 2005); United States v. Steiger, 318 F.3d 1039, 1045 (11th Cir. 2003); United States v. Jarrett, 338 F.3d 339, 345 (4th Cir. 2003); United States v. Grimes, 244 F.3d 375, 383 (5th Cir. 2001).

government purchase enough to suggest that the ISP was coerced into collecting user data.

2. Did the Government "Induce" the Data Brokers to Sell Data Packages?

As established above, *Maryland v. Macon* articulates that a government purchase does not render a seller's actions involuntary. Thus, *Macon* established that voluntary post-hoc transactions do not ordinarily convert willing sellers into state actors.[95] There is good reason behind this doctrine: if the Fourth Amendment regulated every open-market transaction, then *every time* a private party contracts with the government, they would become a state actor. Furthermore, as established above, there is no reason to doubt that brokers sell data packages to the government voluntarily, given individual brokers stand to profit enormously.

However, it is "axiomatic that a state may not induce, encourage or promote private persons to accomplish what it is constitutionally forbidden to accomplish."[96] Can the prospect of a huge windfall count as "inducement" for Fourth Amendment purposes? What happens if the government becomes a routine and systematic purchaser of such information, such that the service provider can reliably depend on government purchases to sustain their business? Under the inducement principle, the government can transform private parties into state actors not only "when it has exercised coercive power," but also when it "has provided such significant encouragement . . . that the choice must in law be deemed to be that of the State."[97] Could the prospect of consistent profits due to government purchases provide "significant encouragement" rising to the level of inducement?

Even if the government were a systematic, monopsonist buyer of data that exerted serious power over brokers, economic inducement does not amount to "coercion" or "significant encouragement" needed to trigger Fourth Amendment scrutiny.[98] Courts have declined to recognize that free market forces can *ever* create inducement sufficient to invoke constitutional protections—even if private actors are *actually* bending to government preferences and changing their behavior accordingly. For example, bounty

95. Maryland v. Macon, 472 U.S. 463 (1985).

96. Norwood v. Harrison, 413 U.S. 455, 465 (1973).

97. Blum v. Yaretsky, 457 U.S. 991, 1004 (1982).

98. *Id.*

systems have been upheld as valid (*i.e.*, held not to be considered state action) in the Supreme Court and most circuits.[99] Yet these systems more directly involve economic inducement: the (legal) market exists solely because the government is a buyer, and yet the Fourth Amendment does not protect against searches and seizures by bounty hunters. Bounty systems have been upheld as legitimate largely because the relationship arises out of a bounded contract rather than "legislative fiat," suggesting that for compulsion to occur, it must be akin to legislative fiat.[100] Economic inducement certainly does not qualify under this criterion. Similarly, "private corporations whose business depends primarily on [government] contracts to build roads, bridges, dams, ships, or submarines" do not qualify as state actors either; their actions "do not become acts of the government by reason of their significant or *even total engagement* in performing public contracts."[101] Thus, a voluntary post-hoc transaction, like a broker's sale of data to the government, cannot induce or otherwise create state action.

3. Does the Service Provider Fulfill a "Public Function"?

This section has established that ISPs and data brokers do not qualify as state actors, because the government is not involved in the initial collection, and because the prospect of a government purchase does not "induce" private actors for state action purposes. However, courts have held that private actors can be subject to the Bill of Rights even when there is no government entanglement in the initial collection activity. Under the "public function doctrine," private actors are subject to the Fourth Amendment when they perform public functions ordinarily reserved for government. For example, in *Marsh v. Alabama*, the Court reasoned a privately-owned municipality was sufficiently analogous to a public town and subjected it to constitutional restrictions on state action. Thus, the town could not

99. Taylor v. Taintor, 83 U.S. 366, 372 (1872); Ouzts v. Md. Nat'l Ins. Co., 505 F.2d 547, 549-50 (9th Cir. 1974). *See generally* Andrew D. Patrick, *Running from the Law: Should Bounty Hunters Be Considered State Actors and thus Subject to Constitutional Restraints?*, 52 VAND. L. REV. 171 (1999) (explaining the doctrinal basis for upholding bounty systems in the circuits).

100. Taylor v. Taintor, 83 U.S. 366 (1872); *see also* Ouzts v. Md. Nat'l Ins. Co., 505 F.2d 547, 549-50 (9th Cir. 1974) (Reaffirming *Taylor*'s central holding that "the common law right of the bondsman to apprehend his principal arises out of a contract between the parties and does not have its genesis in statute or legislative fiat.").

101. Rendell-Baker v. Kohn, 457 U.S. 830, 841 (1982) (emphasis added).

prosecute a Jehovah's Witness for distributing religious pamphlets without implicating the First Amendment.[102]

Similarly, service providers might be said to assume a public function: surveillance. Courts, however, have generally applied the public function doctrine in extremely narrow circumstances. A private party satisfies the doctrine only where it usurps a power "traditionally exclusively reserved to the State [or other government actor]."[103] The Supreme Court has stressed that what cases under "the public-function doctrine have in common [is] the feature of exclusivity."[104] Yet "[w]hile many functions have been traditionally performed by governments, very few have been 'exclusively reserved to the State.'"[105] Education, for example, is not "exclusively reserved to the State," for private schools have also served this public function.[106] Indeed, "no functions other than conducting elections for public office and running an entire town have been deemed to qualify."[107] While policing would appear to be a public function exclusively reserved to the state, "the history of public policing is virtually inseparable from the history of private policing."[108] As a result, "no aspect of policing, neither patrol nor detection, has ever-been 'exclusively' performed by the government, and all have at one point or another, been left largely to private initiative."[109] This includes surveillance. Private parties (for example, store owners) have historically hired private detectives "to spy on[] everyone from insurance claimants and litigation opponents to employees, business partners, and even prospective neighbors."[110] Surveillance, though a public function, was arguably not "exclusively reserved to the State."[111] Service providers, then, may not satisfy the public function test.

But even if surveillance was exclusively reserved to the State, courts decline to find government action unless there is *complete* usurpation of a public function by the private sector. *Marsh*, for example, involved a

102. 326 U.S. 501 (1946).

103. Jackson v. Metropolitan Edison Co., 419 U.S. 345, 352 (1974).

104. Flagg Bros. v. Brooks, 436 U.S. 149, 159 (1978).

105. *Id.* at 158.

106. Rendell-Baker v. Kohn, 457 U.S. 830, 842 (1982).

107. David A. Sklansky, *The Private Police*, 46 UCLA L. REV. 1165, 1257–58 (1999).

108. *Id.* at 1259.

109. *Id.*

110. *Id*. at 1176.

111. Flagg Bros. v. Brooks, 436 U.S. 149, 158 (1978).

complete private usurpation of all municipal functions of a privately-owned town: "Gulf Shipbuilding Corp. performed all the necessary municipal functions in the town of Chickasaw, Ala., which it owned."[112] The Supreme Court recounted that, in other public function cases, "the Texas Democratic Party in *Smith* and the Jaybird Democratic Association in *Terry* effectively performed the *entire* public function of selecting public officials."[113] *Marsh* further suggests that a private actor is only to be treated as a state actor when it has "taken on all the attributes of a town [or other government actor]."[114]

By contrast, ISPs and data brokers have not completely usurped government surveillance by any stretch of the imagination. The government still seeks warrants for location-tracking.[115] For the public function doctrine to apply, there would have to be virtually no government-conducted surveillance, and geolocation surveillance would have to be conducted exclusively by acquisitions of data collected by ISPs.

If agencies merely purchase data from brokers on an ad-hoc basis, it can hardly be said that the private sector has usurped a public function. However, if the government begins to *routinely* and *systematically* purchase data from brokers, and dramatically decreases its own surveillance activities, it *might* then begin to resemble the public function doctrine. But until the providers completely usurp the government's surveillance function, or until the government openly directs the ISPs to collect records on specific people, state action doctrine will not apply. A purchase of data therefore remains untouched by the Fourth Amendment.

* * *

Consequently, when the government purchases data packages from third-party brokers, no government search occurs. The purchase itself is not state action, nor does it convert the initial collection or sales of user data into state action cognizable by the Fourth Amendment. Nor can the ISP's initial collection of data be said to fulfill a public function that the government has abdicated.

---

112. *Id.* at 159 (citing Marsh v. State of Ala., 326 U.S. 501 (1946)).

113. *Id.* (emphasis added).

114. *Id.* at 159 (quoting *Amalgamated Food Emp. Union Loc. 590 v. Logan Valley Plaza, Inc.*, 391 U.S. 308, 332 (1968) (Black, J., dissenting)).

115. *See, e.g.*, United States v. Pickens, 58 F.4th 983 (8th Cir. 2023); United States v. Rubin, No. 322CR00012MMDCSD1, 2023 WL 3044579, at *1 (D. Nev. Apr. 21, 2023); United States v. Sconiers, No. 1:21-CR-00267 JLT, 2023 WL 425818 (E.D. Cal. Jan. 26, 2023).

Even assuming users have a reasonable expectation of privacy in the records sold by brokers, then, government purchases of data fall outside the bounds of the Fourth Amendment—because, at most, a mere private search has occurred. Thus, the government need not obtain a warrant to purchase data *regardless* of whether users have a reasonable expectation of privacy in their commercially available data.

II. USERS' REASONABLE EXPECTATION OF PRIVACY

Part I establishes that agencies need not obtain a warrant to purchase sensitive geolocation data. This Note nevertheless proposes that users *do* have a reasonable expectation of privacy in the records being sold to government agents, suggesting a disconnect between the spirit of the Fourth Amendment and its protections under current precedent.

Though state action doctrine is dispositive on the constitutional question, it is important to proceed with an inquiry into users' reasonable expectations of privacy—the second step of the Fourth Amendment test—for several reasons. First, this analysis of purchasing data under the Fourth Amendment would be incomplete without an account of users' reasonable expectation of privacy. While all existing scholarship on purchases of data hinge solely on the *Katz* test, no piece has yet been fully or comprehensively accurate in its privacy analysis. Crucially, no scholarship has addressed, in depth, the argument of agency lawyers as to why these purchases do not invade people's privacy rights: information that is commercially available *cannot* reasonably be believed to be private since it can be bought by anyone. This Note is the first piece to respond to this argument in detail. Additionally, the conclusion that users do have a reasonable expectation of privacy in their geolocation data demonstrates that, but-for the state action problem, this data would constitute exactly the type of private information that the courts have interpreted the Fourth Amendment to protect. This tension underscores the need to affirmatively protect users' privacy rights.

This Part first demonstrates that under *Carpenter v. United States* and *Kyllo v. United States*, users have a reasonable expectation of privacy in their geolocation records even if these records are commercially available. Second, it advances that users do not consent to a search by signing data-sharing Terms of Service (ToS) agreements, nor can ISPs or data brokers consent to a search on users' behalves. But for the state action problem, then, users would retain constitutional privacy rights in these records.

Establishing that users have a reasonable expectation of privacy in their records under the Constitution consequently establishes that there ought to be *some* data privacy protections even if they do not stem from the Fourth Amendment. This suggests that Congress (and, in the interim, agencies)

ought to step in to fill the gap left by the Fourth Amendment due to the state action problem.

A. Establishing a Reasonable Expectation of Privacy in Commercial Data: Carpenter and the Third-Party Doctrine

Carpenter, the Supreme Court's latest pronouncement on the Fourth Amendment in the information age, firmly establishes that users have a reasonable expectation of privacy in the records created on them that are ultimately sold to the government. Petitioner Timothy Carpenter was suspected as an accomplice to a series of robberies, and under the Stored Communications Act (SCA), a prosecutor obtained two court orders to compel Carpenter's cellphone records from his wireless carriers. The first of these orders compelled seven days of Carpenter's CSLI data from Sprint, and the second turned up 127 days of CSLI data from MetroPCS.[116]

Importantly, court orders under the SCA require mere "reasonable grounds" that the records "are relevant and material to an ongoing criminal investigation"[117]—a "showing [that] falls well short of the probable cause required for a warrant."[118] The core question in *Carpenter*, then, was whether the government needed a warrant to procure these records. The Supreme Court answered in the affirmative: *both* the seven-day and 127-day CSLI records were protected by a reasonable expectation of privacy.

Carpenter represents a departure from established Fourth Amendment doctrine. Long-standing precedent suggests that "a person has no legitimate expectation of privacy in information he *voluntarily* turns over to third parties."[119] Under this "third-party doctrine," people lose any reasonable expectation of privacy in incriminating information that is freely revealed

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

117. 18 U.S.C. § 2703(d).

118. *Carpenter*, 138 S. Ct. at 2221.

119. Smith v. Maryland, 442 U.S. 735, 743-44 (1979) (emphasis added).

to other people, whether they are strangers[120] or business associates[121]—even if they intended their conversations to be private.[122]

When users carry their phones to different places, ISPs contemporaneously trace and document their locations in extensive geolocation records.[123] In one sense, then, users like Timothy Carpenter voluntarily convey their location information to a third party when they use their phones. Under the third-party doctrine, they ought to lose their reasonable expectation of privacy. The Supreme Court held as much in the context of at least certain kinds of metadata. In *Smith v. Maryland*, for example, the authorities installed a pen register in a suspect's phone to record all numbers dialed from that phone. Because phone companies create records on the numbers that any given telephone dials, users were conveying those metadata to the phone companies—a third party. As a result, the Court held the government's use of a pen register was not a "search."[124]

Four decades later, *Carpenter* declined to apply *Smith*'s third-party doctrine to historic CSLI data collected over the course of seven days.[125] The Court reasoned that even if people know their phones convey their locations to ISPs, using cellphones is inescapable. Phones are "'such a pervasive and insistent part of daily life' that carrying one is indispensable to participation in modern society."[126] Therefore, people do not "voluntarily" "assume the risk" that their private information would be disclosed simply by using their

120. *See generally* United States v. White, 401 U.S. 745 (1971) (applying doctrine in context of supposed strangers in a drug deal who turned out to be government agents).

121. *See generally* Hoffa v. United States, 385 U.S. 293 (1966) (applying doctrine in context of business associates who turned out to be government informants).

122. *See White*, 401 U.S. at 749 (quoting *Hoffa*, 385 U.S. at 302) (noting that just because someone had a "misplaced belief" that someone would not reveal what they were told does not render their admission involuntary).

123. Shenkman, *Legal Loopholes and Data for Dollars*, CTR. FOR DEM. & TECH. (2021).

124. 442 U.S. 735 (1979).

125. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) ("We therefore decline to extend *Smith* and *Miller* to the collection of CSLI.").

126. *Id.* at 2220 (citing Riley v. California, 573 U.S. 373, 385 (2014)).

phone.[127] Finding that there was a reasonable expectation of privacy, the Court held that a search occurred when the government compelled the ISP to hand over CSLI data.

Users bear an equally reasonable expectation of privacy over the records sold by data brokers. There is no reason to suspect that a user's expectation of privacy changes depending on whether the government obtained those records via purchase or via *Carpenter*-style compulsion. Crucially, the fact that these data are commercially available does not obviate a user's reasonable expectation of privacy, either.

1. Applying Carpenter

Data brokers sell the same historic CSLI data contemplated in *Carpenter* to governments in large, anonymized data packages;[128] anonymized data packages, however, can easily be deanonymized.[129] These CSLI packages, like the historic data compelled in *Carpenter*, involve at least a week's worth of data—and usually track much longer periods.[130] Whether the government purchases those data or compels ISPs to hand it over (as in *Carpenter*), users make their information equally available to a third party: the service provider. Thus, there is no reason to distinguish people's reasonable expectation of privacy based on whether the government purchases or compels the ISP to obtain the same data.

While historic geolocation data represents virtually the entire market of (reported) law enforcement and intelligence agency purchases,[131] not all

127. *Id.* ("Apart from disconnecting the phone from the network, there is no way to avoid leaving behind a trail of location data. As a result, in no meaningful sense does the user voluntarily 'assume[] the risk' of turning over a comprehensive dossier of his physical movements.").

128. Tokson, *supra* note 29.

129. Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data [https://perma.cc/9WLV-R2S8]; Kelsey Campbell-Dollaghan, *Sorry, Your Data Can Still Be Identified Even if it's Anonymized*, FASTCOMPANY (Dec. 10, 2018), https://www.fastcompany.com/90278465/sorry-your-data-can-still-be-identified-even-its-anonymized [https://perma.cc/86FM-9K68].

130. Ng, *supra* note 10; Shenkman et al., *supra* note 5.

131. Shreya Tewari & Fikayo Walter-Johnson, *New Records Detail DHS Purchase and Use of Vast Quantities of Cell Phone Location Data*, ACLU (July 18, 2022),

location data packages are of CSLI. Do users have a reasonable expectation of privacy over non-CSLI geolocation data? Formally speaking, *Carpenter*'s holding applies strictly to historic CSLI data collected over the course of at least seven days. The Court underscored that "[o]ur decision today is a narrow one. We do not express a view on matters not before us."[132] That said, given that other geolocation data is just as invasive[133]—and is conveyed just as involuntarily—as CSLI data, *Carpenter*'s holding ought to extend. Indeed, Dori Rahbar's Note in the *Columbia Law Review* ably chronicles how lower courts have uniformly extended *Carpenter*'s holding to acquisitions of non-CSLI geolocation data, chiefly location data collected by phone-based applications and ISPs.[134]

What if data brokers sell non-location information to law enforcement? While reported agency purchases of data involve geolocation information,[135] it bears mentioning that data brokers sell other kinds of data to private actors as well. Brokers sell credit card purchase histories, social media data, demographic information, and mental health data to advertisers and other private parties—and could eventually sell to the government.[136]

---

https://www.aclu.org/news/privacy-technology/new-records-detail-dhs-purchase-and-use-of-vast-quantities-of-cell-phone-location-data [https://perma.cc/8Z6N-BHH5]. *See generally* Shenkman et al., *supra* note 5 (describing how law enforcement agencies buy data from brokers).

132. *Carpenter*, 138 S. Ct. at 2220.

133. *See* Rahbar, *supra* note 36, at 726-41 (collecting cases in lower courts suggesting non-CSLI geolocation data is just as invasive as CSLI).

134. *Id*.

135. *See, e.g.*, Laura Hecht-Felella, *Federal Agencies Are Secretly Buying Consumer Data*, BRENNAN CTR. (Apr. 16, 2021), https://www.brennancenter.org/our-work/analysis-opinion/federal-agencies-are-secretly-buying-consumer-data [https://perma.cc/6QWJ-UGJ2]; Corin Faife, *Feds Are Tracking Phone Locations with Data Bought from Brokers*, THE VERGE (July 28, 2022), https://www.theverge.com/2022/7/18/23268592/feds-buying-location-data-brokers-aclu-foia-dhs [https://perma.cc/9PUJ-Q27S]; Cyphers, *supra* note 24.

136. Joanne Kim, *Data Brokers and the Sale of Americans' Mental Health Data*, DUKE SANFORD CYBER POL'Y PROGRAM (Feb. 2023), https://techpolicy.sanford.duke.edu/wp-content/uploads/sites/4/2023/02/Kim-2023-Data-Brokers-and-the-Sale-of-Americans-Mental-Health-Data.pdf [https://perma.cc/7KQN-AZ97].

Given the narrowness of *Carpenter*'s holding, whether users have a reasonable expectation of privacy in those records turns on the nature of the specific kind of data being purchased. The Court expressly declined to overrule *Smith v. Maryland*,[137] which means that the third-party doctrine still applies to some metadata (e.g., pen registers) in a way it does not apply to CSLI data. Nevertheless, if brokers begin to sell certain categories of sensitive information to the government—like biomedical data, financial records, and the contents of communications—there is good reason to suspect such sales of mass data will soon be governed by *Carpenter*. Lower courts have routinely suggested the contents of communications and biomedical information are firmly protected by a reasonable expectation of privacy.[138] Additionally, most significant lower court cases that uphold *Smith v. Maryland*'s application of the third-party doctrine to sensitive data predate *Carpenter*.[139]

Carpenter's potential embrace of the "mosaic theory" of the Fourth Amendment further suggests that even mass sales of other less-sensitive data (say, purchase histories) may be protected by a reasonable expectation of privacy.[140] At its core, the mosaic theory asks "whether a series of acts that are not searches in isolation amount to a search when considered as a group."[141] Though the briefings for *Carpenter* hinged explicitly on the mosaic theory, the Court at no point grounds its opinion in the theory. That said, the Court stressed that the entire CSLI record, collected "over the

137. *Carpenter*, 138 S. Ct. at 2220 (stating that the Court "do[es] not disturb the application of *Smith* and *Miller* or call into question conventional surveillance techniques").

138. *See generally* Rahbar, *supra* note 36 (collecting cases).

139. The District Court for the District of Columbia, for example, attempted to distinguish bulk collection of metadata from *Smith*. Klayman v. Obama, 957 F. Supp. 2d 1 (D.D.C. 2013), *vacated and remanded*, 800 F.3d 559 (D.C. Cir. 2015). But the D.C. Circuit reaffirmed that *Smith* remains controlling over bulk metadata collection. Klayman v. Obama, 805 F.3d 1148, 1149 (D.C. Cir. 2015). ("The Government's collection of telephony metadata from a third party such as a telecommunications service provider is not considered a search under the Fourth Amendment, at least under the Supreme Court's decision in *Smith v. Maryland* . . . . That precedent remains binding on lower courts in our hierarchical system of absolute vertical *stare decisis*."). Both these decisions took place prior to *Carpenter*.

140. Orin Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311 (2012).

141. *Id.* at 320.

course of 127 days," created "an all-encompassing record of the holder's whereabouts" and "near perfect surveillance."[142] This is only possible if every CSLI datapoint is put in conversation with the others and viewed in the aggregate. This might suggest that "the Court . . . accept[ed] the mosaic theory by considering the data presented as a group."[143]

A similar logic applies to all other kinds of data. When the Court decided *Smith* in 1979, the pen register in question was only able to reveal limited and discrete information: numbers dialed on a single landline.[144] Surveillance technology since then has evolved to near-omnipotence. While a single piece of data might not reveal much alone, when put together with other smaller, discrete collections, it can paint a comprehensive picture of a person's habits and private activities.[145] As brokers venture to sell other kinds of mass data, if those data have the capacity to reveal information like people's sexual orientation, political practices, religious affiliations, locations, and other details of their private lives, courts may be more likely to apply *Carpenter* to find a reasonable expectation of privacy.

As it stands, because the vast majority of (reported) sales of data packages to law enforcement and intelligence agencies involve large swaths of historic geolocation data, *Carpenter* applies, and users have a reasonable expectation of privacy.

2. Do Users Have a Reasonable Expectation of Privacy in Commercially Available Data?

In internal memoranda authored by government attorneys, agencies have primarily contended that they should be able to purchase geolocation

142. *Carpenter*, 138 S. Ct. at 2217; *see also* Taylor Wilson, Note, *The Mosaic Theory's Two Steps: Surveying* Carpenter *in the Lower Courts*, 99 TEX. L. REV. ONLINE 155, 155 (pointing out that the *Carpenter* Court focused on the nature of information that CSLI conveys).

143. Wilson, *supra* note 142, at 156; *see also* Ken Wallentine, *Tuggle's Losing Struggle with the Mosaic Theory of the Fourth Amendment*, LEXIPOL (July 15, 2021) ("To me, it appears that the mosaic theory holds sway with at least some of the Supreme Court justices [in *Carpenter*]."); Ben Vanston, Note, *Putting Together the Pieces: The Mosaic Theory and Fourth Amendment Jurisprudence since* Carpenter, 124 W. VA. L. REV. 658, 671 (2022) ("The Court, in its conclusion, seemingly endorsed the mosaic theory of the Fourth Amendment; however, it does not explicitly state the proposition.").

144. *See* Smith v. Maryland, 442 U.S. 735 (1979).

145. *See* Kerr, *supra* note 140, at 335.

data packages without restriction because these packages are commercially available.[146] The Defense Intelligence Agency, for example, "does not construe the *Carpenter* decision to require a judicial warrant endorsing purchase or use of commercially available data for intelligence purposes."[147] That private actors can purchase these data, it is reasoned, suggests that users cannot expect privacy in these records.[148]

This argument is grounded in serious functional considerations: if foreign governments and private institutions can access these data for debatably nefarious purposes, why should U.S. national security agencies be inhibited from accessing these data? As much as this might make sense, doctrinally, the Fourth Amendment suggests that the mere commercial availability of the data would *not* disrupt users' reasonable expectation of privacy. (For an extended discussion of a better way to balance civil liberties concerns with foreign threat vulnerabilities, see Section III.C.)

The agency lawyers' theory has roots in *Kyllo v. United States*.[149] *Kyllo* identifies when a piece of information may be considered "exposed to public view" in the context of commercially available surveillance methods.[150] In that case, police used a thermal detection device to determine if a person's home exhibited unique heat signatures indicative of illegal marijuana growth. The Court held that this "constitute[d] a search" partly because the device used to obtain the information was "not in general public use."[151] Importantly, *Kyllo* was an application of "[t]he *Katz* test—whether the individual has an expectation of privacy that society is prepared to

146. Tokson, *supra* note 29.

147. Savage, *supra* note 28.

148. *See also* Akhil Amar, *"I Always Feel Like Somebody's Watching Me": A Fourth Amendment Analysis of the FBI's New Surveillance Policy*, FINDLAW BLOG (June 14, 2002), https://supreme.findlaw.com/legal-commentary/i-always-feel-like-somebodys-watching-me.html [https://perma.cc/GSN2-SPAS] (suggesting where a private actor may obtain certain kinds of data unfettered, the Fourth Amendment should not require the government to obtain a warrant to access these data).

149. Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 [https://perma.cc/G7GR-5797]; *see also* Tokson, *supra* note 29 (asserting *Kyllo* would govern this line of argument).

150. Kyllo v. United States, 533 U.S. 27, 34 (2001).

151. *Id.* (quoting *Silverman v. United States*, 365 U.S. 505, 512 (1961)).

recognize as reasonable."[152] Thus, lower courts have consistently extrapolated that when a surveillance technique is in general public use, people have a diminished expectation of privacy in the information the technique reveals.[153]

Even though brokers make data packages commercially available, the relevant inquiry is whether sensitive data purchases are in "general public use." Tokson argues that these sensitive data packages are "functionally private" because they are stored in big anonymized blocks when *not* in government hands.[154] "[V]endors who sell such data often do so either exclusively to law enforcement agencies or in large anonymized chunks to other marketing companies for use in automated advertising."[155] Indeed, when selling to advertisers and other private institutions, brokers sell large, aggregated, and anonymized chunks of mass data.[156] Data sold to private parties are at the "census block level" to help advertisers ascertain trends rather than individual-level information.[157] But when data packages are sold to government buyers, these data are (reportedly) deanonymized (some of the time).[158] This fact is critical: the applications and privacy implications of deanonymized (or even anonymized) individual-level data differ dramatically from aggregated blocks of anonymized data.[159] As a

152. *Id.*.

153. *See, e.g.*, United States v. Katzin, 732 F.3d 187, 238 (3d Cir. 2013), *reh'g en banc granted, opinion vacated*, No. 12-2548, 2013 WL 7033666 (3d Cir. Dec. 12, 2013), *and on reh'g en banc*, 769 F.3d 163 (3d Cir. 2014) ("*Kyllo* made much of the fact that the technology used in that case was 'not in general public use.' Alternatively, GPS technology is widespread, and one need look only on the dashboard of his vehicle or the screen of his cellular telephone to spot one. Kyllo's concerns, of course, arise in all Fourth Amendment cases dealing with advanced technology. But it is safe to say that those concerns are not implicated by our facts.").

154. Tokson, *supra* note 29.

155. *Id*.

156. Tokson, *supra* note 29; Valentino-DeVries, *Your Apps Know Where You Were*, *supra* note 40; *Home Page*, SECURUS, https://securustech.net/ [https://perma.cc/Q3JF-FXD8].

157. Cox, *Data Broker Is Selling Location Data*, *supra* note 4.

158. Tokson, *supra* note 29; Valentino-DeVries, *Your Apps Know Where You Were*, *supra* note 40.

159. *Id. But see* Sophie Bushwick, *"Anonymous" Data Won't Protect Your Identity*, SCIENTIFIC AM. (July 23, 2019), https://www.scientificamerican.com

result, the product sold to the government and advertisers might properly be characterized as different—meaning that deanonymized dataset purchases are *not* in general public use.

Law enforcement agencies, however, reportedly purchase anonymized datasets as well.[160] Are *anonymized* data packages in general public use? Even when individual user data is nominally anonymized, a New York Times report revealed that user location data can easily be deanonymized with just a few corroborating data points.[161]

Even setting aside the ease with which anonymized datasets can be deanonymized, purchases of anonymized packages would be difficult to characterize as in "general public use." Admittedly, advertisers—private actors—are major buyers in the data broker market, routinely purchasing the packages also sold to government clients.[162] Brokers, however, do not sell to ordinary people: they sell to private *institutions*, not natural people. Thus, "[y]ou and I generally cannot purchase location tracking data on our fellow citizens from these vendors."[163]

The critical question that Tokson overlooks is whether something that is commercially available (i.e., anonymized data) but only purchased and used by big companies can qualify as being in "general public use." No circuit courts have directly opined on this issue. Nor does *Kyllo* provide much guidance: as the dissent complains, "how much use is general public use is not even hinted at by the Court's opinion."[164]

Nevertheless, there is good reason to doubt that anonymized dataset purchases are in general public use. Whether something is "expose[d] to the public" depends "not upon the theoretical possibility, but upon the actual

---

/article/anonymous-data-wont-protect-your-identity/ [https://perma.cc/8665-4QXM] (Suggesting anonymized data can quickly and easily be deanonymized).

160. Bennett Cyphers, *Inside Fog Data Science*, ELEC. FRONTIER FOUND (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/08/inside-fog-data-science-secretive-company-selling-mass-surveillance-local-police [https://perma.cc/36VC-JCQ9].

161. Valentino-DeVries, *Your Apps Know Where You Were*, *supra* note 40.

162. Zack Whittaker, *Data Brokers Track Everywhere You Go, But Their Days May Be Numbered*, TECHCRUNCH (July 9, 2020), https://www.techcrunch.com/2020/07/09/data-brokers-tracking/ [https://perma.cc/SMQ8-TRYP].

163. Tokson, *supra* note 29.

164. *Kyllo*, 530 U.S. at 47.

likelihood, of discovery by a *stranger*."[165] Only if a random *stranger* could realistically purchase those records, then, would data packages for sale qualify as being in "general public use."[166] This suggests the "general public use" inquiry centers not on mere commercial availability to extremely wealthy institutional actors, but instead, the realistic likelihood that an ordinary person would happen upon such information. Because brokers sell to institutional buyers rather than individuals, and because data packages are prohibitively expensive for most,[167] there is only a theoretical possibility that these data are exposed to the public. As a result, the commercially available nature of data packages does not defeat users' reasonable expectation of privacy.

This calculus may change if a single institutional buyer purchases a data package and sells individuals' data at a more affordable rate to the general public. In the context of facial tracking technology, one company purchased ClearView AI and allowed individuals to conduct a single search of the database at a fixed, affordable rate—effectively turning ClearView AI, which normally targets institutional customers, into a retail product.[168] Even just

165. United States v. Maynard, 615 F.3d 544, 560 (D.C. Cir. 2010) (quoting *Katz*, 389 U.S. at 351); United States v. Gbemisola, 225 F.3d 753, 759 (D.C. Cir. 2000).

166. *Maynard*, 615 F.3d at 560 (quoting *Kyllo*, 530 U.S. at 34).

167. Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600 [https://perma.cc/DR9E-GL47]. Note that some lower court decisions might at first suggest that merely because something is expensive does not mean it is not in "general public use." However, lower courts have held this to be the case in the context of expensive surveillance cameras in the thousands of dollars. *See, e.g.*, United States v. Rivera-Alejandro, 2014 WL 12922962 (D.P.R. Apr. 3, 2014), *report and recommendation adopted*, 2014 WL 12922963 (D.P.R. May 14, 2014) (finding an 800mm "camera, lens, and camcorder used are not highly sophisticated devices unavailable for general public use" even though it had a "high price" of $6,000); United States v. Van Damme, 48 F.3d 461, 463 (9th Cir. 1995) ("A 35 mm camera with a 600 mm lens is a kind of vision enhancer commonly available to the public."); United States v. Tuggle, 4 F.4th 505, 516 (7th Cir. 2021) (finding "the isolated use of pole cameras here did not run afoul of Fourth Amendment protections" because "cameras are in 'general public use,'" in spite of its multi-thousand dollar price point).

168. Drew Harwell, *Clearview AI to Restrict Sales of Recognition Tool*, WASH. POST (May 9, 2022), https://www.washingtonpost.com/technology/2022/05/09/clearview-illinois-court-settlement [https://perma.cc/K6WG-5GPT].

a single seller in the market, then, might convert these functionally private data packages into a technique in "general public use," thereby shattering the reasonable expectation of privacy.

B. Privacy Persists: No Consent to Searches

Even though *Carpenter* establishes users' reasonable expectation of privacy, it is possible for them to waive their privacy rights and consent to a search. First, when users use phone-based applications that track their location, they often accept Terms of Service ("ToS") Agreements (via a pop-up button, or toggling location services) that expressly state that their data may be shared with "trusted third-parties."[169] Scholars assert that circuits are split over whether signing ToSs with these terms constitutes consent to a search.[170] However, this Note suggests that existing case law is consistent and compels the same conclusion: for a ToS to constitute a waiver of privacy expectations, specific and detailed notice that user data may be sold to the government is required. Generic data-sharing provisions cannot reach this demanding standard.

Alternatively, could ISPs or data brokers consent to a search of these records on the user's behalf? ISPs and data brokers hold equal and common authority over the records sold to the government. On this basis, Orin Kerr advances a novel theory premised on third-party consent: ISPs, brokers, and users have equal power to consent to a search of the records. Though creative, this theory is inaccurate. Brokers and ISPs do not share common authority over the users' records, because third-party consent is premised on the *users*' voluntary assumption of the risk that ISPs or brokers might authorize a search. As a consequence, these institutional actors cannot consent to a search on the users' behalf.

1. Do Users Consent to Searches via Terms of Service Agreements?

To use certain phone applications, users must accept ToS agreements that expressly provide that their data might be shared with and sold to

169. Lazarus, *supra* note 70; Zach Whittaker, *Meet the Shadowy Tech Brokers that Deliver Your Data to the NSA*, ZD NET (Sept. 5, 2014), https://www.zdnet.com/article/meet-the-shadowy-tech-brokers-that-deliver-your-data-to-the-nsa [https://perma.cc/D7CX-2JAG].

170. *See, e.g.*, Orin Kerr, *Terms of Service and Fourth Amendment Rights*, U. PA. L. REV. 12 (forthcoming 2023), https://ssrn.com/abstract=4342122.

"trusted third-parties."[171] These ToSs manifest as a "single click-through" in response to which users must click "accept" or simply toggle a button.[172] For example, to use popular rideshare or navigation applications, users must toggle the location services button, which in turn gives permission to share data with third-parties.[173] For other, non-location-based phone applications, people reflexively click through ToSs that might contain data-sharing provisions.[174] Indeed, generic ToSs on phone-based applications provide that user information may be shared with "trusted third-parties," with some specifying that user data may be shared in compliance with government requests.[175] But few, if any, specifically provide that user data may be sold to government bodies.[176]

The question is whether reflexively accepting these ToSs amounts to a waiver of privacy rights, and thus consent to a government search. While not raised in *Carpenter*, lower courts have begun to address this question in the context of sharing the contents of communications with law enforcement. Though the doctrine is emerging, the best reading of the law is that ToSs need to give users sufficient notice that the acceptance of the terms may trigger a buying-and-selling chain reaction. On this understanding, generic data-sharing provisions cannot amount to a waiver

171. Lazarus, *supra* note 70; Whittaker, *supra* note 169.

172. Lauren Goode, *App Permissions Don't Tell Us Nearly Enough About Our Apps*, WIRED (Apr. 14, 2018), https://www.wired.com/story/app-permissions [https://perma.cc/2JM9-UJRB].

173. *Id.*

174. *See, e.g.*, Specht v. Netscape, 306 F.3d 17 (2d. Cir. 2002) (noting that in a case about clickwrap, where non-obvious license terms to download software forced arbitration for any disputes, the "bare act downloading the software did not unambiguously manifest assent to the arbitration provision contained in the license terms").

175. Daniel Thomas, *How Third Parties Contribute to Application Vulnerabilities*, SCMEDIA (July 6, 2022), https://www.scmagazine.com/resource/third-party-risk/how-third-parties-contribute-to-application-vulnerabilities [https://perma.cc/TF4S-JP53]; Matt Milano, *Report: 1 in 2 Android Apps Share User Data With Third Parties*, WEBPRONEWS (Oct. 9, 2022) https://www.webpronews.com/report-1-in-2-android-apps-share-user-data-with-third-parties [https://perma.cc/F3J5-XQ9R]; Bennett Cyphers & Gennie Gebhart, *Behind the One-Way Mirror: A Deep Dive Into the Technology of Corporate Surveillance*, ELEC. FRONTIER FOUND (Dec. 2, 2019) https://www.eff.org/wp/behind-the-one-way-mirror [https://perma.cc/6DHS-JKE8].

176. See discussion *infra* Section II.B.1.

of privacy rights; at the bare minimum, ToSs must specify that user data may be shared with the government.

In cases where courts have ruled that ToSs did not waive privacy rights, the ToSs contemplated did not specify that user data may be shared *with the government*. The Sixth Circuit contemplated a ToS that provided that the ISP may access and share "individual Subscriber information . . . as necessary to protect the Service."[177] This is similar to the ToSs users sign to access different applications on their phone.[178] The Court stressed that the agreement "[did] not diminish the reasonableness of [appellee's] trust in the privacy of his emails."[179] Thus, when the government compelled the company, NuVox, to turn over emails without a warrant, a search occurred.[180] Two district courts followed and expanded on the Sixth Circuit's approach. First, in *United States v. Irving*, the District of Kansas found that a ToS granting Facebook the right to handle and share user data however it saw fit did not mean that Facebook could share the user's communications with the government.[181] In *United States v. DiTomasso*, the Southern District of New York further suggested that "when employees constructively consent to searches by their supervisors, it does not automatically follow that they also consent to searches by law enforcement."[182] Importantly, in none of these cases did the waivers sufficiently "put[] users on notice" that their data may be shared with the government.[183]

177. U.S. v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010).

178. Lazarus, *supra* note 70.; Whittaker, *supra* note 169.

179. *Warshak*, 631 F.3d 266. The Court held this in part because mere access does not imply the power to share information with the government. Providers of previous technology retained similar access without diminishing Fourth Amendment rights. For example, the phone company in the seminal *Katz* case had a right to tap calls, yet that authority did not interfere with Katz's reasonable expectation of privacy. But the Court does not explain why the agreement, which expressly provided the ISP may share information, did not permit them to share such information with law enforcement. Kerr, *supra* note 170 (quoting *Warshak*, 631 F.3d at 287).

180. *Id.* at 282.

181. 347 F. Supp.3d 615 (D.Kan. 2018).

182. United States v. DiTomasso, 56 F. Supp. 3d 584, 593 (S.D.N.Y 2014), *aff'd on different grounds*, 932 F.3d 58 (2d Cir. 2019).

183. *Id.* at 596.

Thus, general information-sharing and handling provisions are not enough to create consent to a government search, for they do not put users on notice. Insofar as a ToS's terms provide merely that information may be shared with a "trusted third party," the waiver does not constitute consent to a search.

But even including in ToS provisions the mere fact that information may end up in government hands may not be enough to create consent to a search. Data-sharing provisions may require sufficient detail about the potential buying-and-selling chain reaction to put users sufficiently on notice. Otherwise, the chain of consent is too attenuated, suggesting users did not agree to what transpired.

This theory has roots in the recent Eastern District of Virginia opinion *United States v. Chatrie*. In *Chatrie*, a user signed a ToS that permitted Google to "save [] and use []" location data in "any Google service where [he was] signed in to give [him] more personalized experiences."[184] Though this ToS expressly warned the user that his location data would be harvested, the *Chatrie* court ruled it could not waive his privacy rights. After all, Google did not sufficiently detail just how extensive the location tracking was to be:

> [C]onsent flow did not detail, for example, how frequently Google would record Chatrie's location (every two to six minutes); the amount of data Location History collects (essentially all location information); that even if he "stopped" location tracking it was only "paused," meaning Google retained in its Sensorvault all his past movements; or, how precise Location History can be (i.e., down to twenty or so meters).[185]

This suggests that ToS agreements must be specific and extensively detailed to put people on notice. To waive a user's privacy in the data brokering context, then, would require the ToS specify that a buying-and-selling chain reaction might occur upon acceptance of its terms. Under this high bar, a majority of phone-based app ToSs—which do not put users on notice of the potential for government purchase of data—could not qualify as consent to a search.[186]

This position is consistent with the decisions of courts that have upheld ToSs as creating consent to a search. These courts only ruled that ToSs

184. United States v. Chatrie, 590 F. Supp. 3d 901, 936 (E.D. Va. 2022).

185. *Id.*

186. Goode, *App Permissions*, *supra* note 172; Cyphers & Gebhart, *Behind the One-Way Mirror*, *supra* note 175; Thomas, *How Third Parties Contribute To Application Vulnerabilities*, *supra* note 175; Milano, *Report*, *supra* note 175.

waived privacy rights because their contractual terms specified the precise circumstances under which user data would be shared with law enforcement. First, in *United States v. Adkinson*, T-Mobile handed user records to the FBI in response to an investigation involving multiple robberies at its stores. The Seventh Circuit ruled that the suspect (a T-Mobile user) waived his privacy rights. That ToS expressly provided that T-Mobile may disclose private information about user accounts "to satisfy any applicable . . . governmental request" that helps "protect [T-Mobile's] rights or interests, property or safety."[187] T-Mobile thus satisfied the ToS's articulated circumstances under which user data could be shared with the authorities, since the data were shared only in response to a criminal investigation. Following this decision, the Pennsylvania Supreme Court considered a ToS between a university's network service and a student user of that network who was alleged to have committed a robbery. The ToS for use of that network provided that the "institution has the right to inspect information stored on its system at any time, for any reason, and users cannot and should not have any expectation of privacy with regard to any data, documents, electronic mail messages, or other computer files created or stored on computers within or connected to the institution's network."[188]

While these general terms alone were not dispositive, the ToS also established that information and communications using that service were "subject at any time to disclosure to institutional officials, *law enforcement*, or third parties" in connection with investigations.[189] The Court held that accepting this latter term constituted specific consent to sharing information. These ToSs, then, only diminished privacy expectations because they expressly provided that user data could be shared with the government under a certain set of circumstances, thereby putting users on notice.

Even if ToSs were written to specify that user data may trigger a chain of sales leading to government acquisition, however, the notice problem persists. Rahbar's student note correctly explains that "[w]hen users consent to location data collection through user agreements (say, by 'reflexively' toggling their 'location services' on) they often have *desperately insufficient notice* that such consent might set in motion a buying-and-selling chain reaction" that ends with user data in law enforcement hands,

187. United States v. Adkinson, 916 F.3d 605, 610 (7th Cir. 2019).

188. Commonwealth v. Dunkins, 263 A.3d 247, 250 (Pa. 2021).

189. *Id.*

because these terms are buried within location services policies.[190] The Southern District of New York case supports Rahbar's assertion: the court held that ToSs can constitute consent to searches only if users are sufficiently *and obviously* put on notice.[191] And importantly, in *Chatrie*, Google was found to have not sufficiently put the user on notice of tracking activities not just because of the contractual terms of the ToS, but also because of the "limited and partially hidden warnings provided by Google."[192] After all, the provision authorizing location-tracking appeared to Chatrie only in "a single pop-up screen."[193]

Similar notice problems abound in the context of data-sharing provisions ToSs, where often a single pop-up can "set in motion a buying-and-selling chain reaction" that means their data "enters the open market, reaches the government, and is used by law enforcement."[194] Indeed, swaths of empirical studies establish that users do not understand the implications of data-sharing provisions.[195] This suggests that ToSs, to actually constitute a consent to search, must clearly and obviously alert users to the possibility that accepting the ToS may trigger a series of sales resulting in government acquisition of user data. These consent-to-share terms, furthermore, must not be buried deep in the bowels of the ToS.

Even if some data are connected to valid ToSs that provide adequate notice to users, aggregation of data across apps virtually guarantees that validly shared data are intermingled with data collected under deficient, generic waivers. Attempting to distinguish said waivers within mass datasets, of course, poses massive administrability concerns. The data that remain, furthermore, may be infinitesimal in comparison to the original size of the data package, given that most ToSs in phone-based applications

190. Rahbar, *supra* note 36, at 737 (emphasis added).

191. *DiTomasso,* 56 F. Supp. 3d at 597 ("In contrast to Omegle's policy, which includes only a passing reference to law enforcement—and which gives no indication of the role Omegle intends to play in criminal investigations—AOL's policy makes clear that AOL intends to actively assist law enforcement.").

192. *Chatrie*, 590 F. Supp. 3d at 936.

193. *Id.*

194. Rahbar, *supra* note 36, at 737.

195. Yael Grauer, *What Are 'Data Brokers,' and Why Are They Scooping Up Information About You?*, VICE (Mar. 27, 2018), https://www.vice.com/en/article/bjpx3w/whatare-data-brokers-and-how-to-stop-my-private-data-collection [https://perma.cc/BQ9Y-TCWL].

contain inadequate, vague data-sharing permissions.[196] For these practical reasons, the mere fact that some ToSs might adequately put users on notice is not enough to defeat users' reasonable expectation of privacy in data packages.

Furthermore, even setting aside textually insufficient contractual provisions, *Carpenter* may even preclude the significance of ToS waivers to privacy expectations altogether. The functionality of many phone-based applications depends on consenting to location services ToSs; otherwise, Uber, Google Maps, and other applications simply cannot work.[197] Yet even other location-agnostic phone-based apps require users to consent to sharing permissions, but will draw location data from navigation applications.[198] Drawing on the logic of *Carpenter*, these ToSs cannot be said to have been accepted voluntarily, given the inescapable need to use one's phone in the modern day. Indeed, the *Chatrie* court confirmed that "unlike in *Carpenter*, Chatrie apparently took some affirmative steps to enable location history": enabling location tracking via a "single pop-up screen."[199] Nevertheless, "those steps likely do not constitute a full assumption of the attendant risk of permanently disclosing one's whereabouts during almost every minute of every hour of every day."[200]

Controversially, one scholar even suggests that ToSs can never create consent to a government search, because "Terms of Service can define relationships between private parties, but private contracts cannot define Fourth Amendment rights."[201] After all, "Fourth Amendment rights are rights against the government, not private parties," which is allegedly true "across the range of Fourth Amendment doctrines, including the 'reasonable expectation of privacy' test, consent, abandonment, third-party consent, and the private search doctrine."[202]

Even if one does not endorse this sweeping objection, there is nevertheless good reason to doubt that the signing of a ToS undermines the

196. Goode, *App Permissions*, *supra* note 172.

197. *Id*. ("[A] ride-hailing app like Uber doesn't work without location information. Reject those permissions, and you'll break functionality."); Rahbar, *supra* note 36, at 736-37.

198. *Id.*

199. *Chatrie*, 590 F. Supp. 3d at 936.

200. *Id.*

201. Orin Kerr, *Terms of Service and Fourth Amendment Rights*, U. PA. L. REV. 2 (forthcoming).

202. *Id.* at 1.

reasonable expectation of privacy or that it amounts to consent to a search, because of the notice issues. Under existing doctrine, a ToS cannot constitute consent to a search unless it specifies that users' information might be shared with the government via a sale. Generic ToSs today do not satisfy this standard.[203]

2. Can Service Providers or Brokers Consent to a Search of the User's Records on Their Behalf?

Conceding that users have a reasonable expectation of privacy, Orin Kerr asserts that ISPs and brokers could nevertheless authorize a search on the user's behalf. He dubs this the "Common Access Theory." According to Kerr, when multiple parties have equal authority to the same shared information, any one of those parties can authorize access. So, either data brokers, service providers, or users who are the subject of data being sold can consent to a search. In his words, "[a] company can sell *Carpenter*-protected records without Fourth Amendment oversight because it has the common authority over the records."[204]

The Common Access Theory derives from doctrine on third-party consent to searches of people's homes. One roommate in a house can authorize the police to search the entire home, even if another roommate would not have consented to a search. As the Supreme Court stated in *Matlock*, "mutual use of . . . property by persons generally having joint access or control for most purposes" gives any one of those people "the right to permit the inspection [of the property] in his own right."[205] Common access, then, empowers third parties to consent to a search on the other cotenant's behalf.

Even if one roommate expressly objects to the police searching their home, if that person is not physically present, the authorities can obtain consent to search from the remaining roommate.[206] *Georgia v. Randolph* suggests that when there is a physically present objector, "widely shared social expectations" would militate against going inside the home.[207] The

203. Goode, *App Permissions*, *supra* note 172.

204. Kerr, *Buying Data*, *supra* note 20, at 5.

205. United States v. Matlock, 415 U.S. 164, 171 n.7 (1974).

206. Fernandez v. California, 571 U.S. 292 (holding that police can obtain consent of a roommate to search a house even where the other roommate expressly refuses to allow a search, if the other roommate is not physically present).

207. Georgia v. Randolph, 547 U.S. 103, 111 (2006).

Court reasoned that when one roommate invites a person into their home but "a fellow tenant stood there saying, 'stay out,' no sensible person would go inside."[208] But when the objecting tenant is not physically present, "social expectations" suggest that people can enter into the house.[209] In the context of data purchase, even if a user is not "present" for a sale of their data, the others that share common access and common authority over those records may authorize a government search.

Kerr marshals support for this point by gesturing at two cases where an employer turned over records of communications that an employee made over work devices—suggesting that if employers were allowed to turn over the information, so too may a data broker. Two circuits ruled that employers had common authority over the employee's records, and could authorize government access.[210] In *Walker v. Coffey*, the Third Circuit held that a university had common access to a defendant's emails sent on a work account and work laptop, and so had the authority to turn over the communications to the Pennsylvania Attorney General.[211] In *U.S. v. Ziegler*, the Ninth Circuit held that an employer could hand over documents evincing an employee's crimes, which were saved on his work laptop. Though the employee had a Fourth Amendment privacy interest, the employer shared common access over the records saved on the laptop.[212] This extinguished the employee's Fourth Amendment rights.

Though creative, Kerr's theory does not apply to the purchase of data. The Supreme Court's pronouncements on third-party consent (in the context of roommates) reflect "that it is reasonable to recognize that any of the co inhabitants has the right to permit the inspection in his own right."[213] But this reasonableness is premised on the fact that the cotenants voluntarily "*assumed the risk* that one of their number might permit the common area to be searched."[214] Thus, common authority exists between roommates over a space because they agreed to live with each other.

208. *Id.* at 113.

209. *Id.* at 121 ("[T]he co-tenant's consent [w]as good against 'the absent, nonconsenting' resident.").

210. U.S. v. Ziegler, 474 F.3d 1184 (9th Cir. 2007); Walker v. Coffey, 905 F.3d 138 (3d Cir. 2018).

211. *Walker*, 905 F.3d 138.

212. *Ziegler*, 474 F.3d 1184.

213. *Matlock*, 415 U.S. at 171 n.7.

214. *Id*. (emphasis added).

Through this voluntary decision, they risked that one of their number might consent to a search.

Ordinary users, by contrast, do not voluntarily "assume[] the risk" that an ISP or broker might sell their records just because they use their phones. As *Carpenter* held, phone usage is so pervasive and necessary to function in the modern world that using one's phone does not amount to a "voluntary" transmission of information to a third-party. Similarly, because phone usage is inescapable, it cannot be said that the users voluntarily "assumed the risk" that the ISP or broker might grant access to the records created on the users. They are forced to accept the risks to use their phone. Tenants of a home, by contrast, can choose other roommates.

The lower court decisions that Kerr references in the context of employers are distinguishable as well. In *Randolph*, the Supreme Court suggested that when one tenant of a house invites a person into their home but "a fellow tenant stood there saying, 'stay out' . . . no sensible person would go inside."[215] However, the Court grounded its decision on the fact that the cotenants do not "fall within some recognized hierarchy, like a household of parent and child or barracks housing military personnel of different grades."[216] There was no "superior and inferior" cotenant in *Randolph*.[217] In *Ziegler*, meanwhile, the Ninth Circuit ruled that an employer could authorize access to employee documents saved on a workplace computer containing evidence of criminal activity: there is a clearly "recognized hierarchy" in the workplace, and certainly, over control of work devices.[218] Similarly, in *Walker*, the university employee used the school's email system that was "controlled and operated by Penn State."[219] Thus, "for purposes of the Fourth Amendment, the emails [that the employers handed over to the authorities] were subject to the common authority of Walker's employer. Walker did not enjoy any reasonable expectation of privacy vis-à-vis Penn State."[220] Employees, then, do not enjoy a reasonable expectation of privacy when using devices or networks obviously owned and managed by their employers. Unlike equal cotenants of a house, employees are subordinate to their employers. Thus, employers may authorize access to

215. Georgia v. Randolph, 547 U.S. 103, 113 (2006).

216. *Id.* at 114.

217. *Id.*

218. *Id.*

219. Walker v. Coffey, 905 F.3d 138, 149 (3d Cir. 2018).

220. *Id.* at 149.

employee communications and documents that were created on work devices and transported across work networks.

By contrast, there is no "recognized hierarchy" between a user and a service provider—certainly not one as clear as the employer-employee relationship. Neither party is superior nor inferior. As a result, a service provider cannot authorize access to a user's records in the same way an employer can.

Some nevertheless may suggest that the property right data brokers have over the user's records authorizes them to consent to a search. *Ziegler*, after all, mentioned that "Ziegler could not reasonably have expected that the computer was his personal property, free from any type of control by his employer."[221] But *Ziegler* did not turn on the fact that the employer could access and create records on user activity. As the Sixth Circuit made clear in *U.S. v. Warshak*, providers of previous technology "retained similar [access and property] rights" without diminishing Fourth Amendment rights.[222] For example, the phone company in the seminal *Katz* case had a right to tap calls and create records on those calls, yet that did not interfere with Katz's reasonable expectation of privacy.[223] Thus, the mere fact that an employer owns employee records on work devices is not enough to conclude common authority over the records: crucial to *Ziegler* and *Walker* is that the employer rests higher on the hierarchical ladder than the employee in the records stored on work devices.

* * *

A search occurs when "an expectation of privacy that society is prepared to consider reasonable is infringed."[224] *Carpenter* establishes a reasonable expectation of privacy in commercially available records, and the decision in *Kyllo*, the signing of waivers, and the Common Access Theory do not suggest otherwise.

However, as established in Part I, this is not dispositive of the inquiry. For the warrant requirement to apply to a purchase of sensitive geolocation data, the government's act of purchasing data itself must constitute a search. Therein lies the core issue for the Fourth Amendment's applicability to this case: the state action problem. Because agency purchases of data do not constitute state action, the Fourth Amendment does not protect against warrantless purchases, even if users have privacy rights in these records.

---

221. U.S. v. Ziegler, 474 F.3d 1184, 1192 (9th Cir. 2007).

222. Kerr, *Terms of Service and Fourth Amendment Rights*, at 12 (quoting U.S. v. Warshak, 631 F.3d 266, 287 (6th Cir. 2010)).

223. *See Id.* (quoting *Warshak*, 631 F.3d at 287).

224. Maryland v. Macon, 472 U.S. 463, 469 (1985).

This result underscores an awkward tension in Fourth Amendment law: even though users bear a reasonable expectation of privacy over their commercial records and the spirit of the Fourth Amendment points to the need for data privacy protections, the state action doctrine decisively cuts against the warrant requirement. While the government cannot obtain users' sensitive geolocation data without a warrant, it could purchase those records without triggering Fourth Amendment protections. In light of this disconnect, Congress must step up and fill this privacy gap.

III. REWIRING THE FOURTH AMENDMENT: THE IMPERATIVE OF CONGRESSIONAL ACTION

This Note's analysis has shown that Fourth Amendment doctrine does not protect against the warrantless purchase of users' sensitive geolocation data. Part III will demonstrate that a core purpose of the Fourth Amendment was to make illegible to the government the very kinds of information that geolocation data reveals.[225] This suggests the need for *some* privacy protections for these data transactions.

Yet, as this Part establishes, attempts to colorfully stretch existing state action doctrine to cover these unfamiliar digital-age circumstances are misguided. A doctrinal shift of this magnitude is not only unlikely, but also affirmatively undesirable.

Relying on the Fourth Amendment as the primary data privacy bulwark or even passing legislation like FAINFSA leaves open a serious intelligence vulnerability. Neither FAINFSA nor the Fourth Amendment prohibit foreign governments from purchasing the very same sensitive geolocation data that U.S. agencies would be forbidden from obtaining without a warrant. Disabling U.S. agencies tasked with protecting national security in this way presents serious foreign threat risks.

Instead, the inapplicability of the Fourth Amendment presents a profound opportunity for Congress to reimagine the way we think about and protect privacy. As a result, this Note calls for Congress to enact privacy legislation that regulates *sales* of people's private data, rather than government *purchases*. This legislation would address the dangers posed by

225. *See* Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101 (2008) (advancing a comprehensive political theory of the Fourth Amendment as protecting personal security and private lives); Daphna Renan, *The Fourth Amendment as Administrative Governance*, 68 STAN. L. REV. 1039, 1050 n.33 (2016) (citing many subsequent sources reaffirming this vision of the Fourth Amendment). This Note advances a similar, but distinguishable, vision of the Fourth Amendment.

data brokers at their source—dangers similar to those that initially inspired the Fourth Amendment.

A. Purchases and the Fourth Amendment's Anti-Persecution Purpose

The Fourth Amendment was designed to prevent persecution by keeping people's private lives (political opinions, religious beliefs, and private activities which could supply the basis for persecution) invisible to the government. Because purchases of location data can reveal precisely these things, there ought to be some privacy protection against mass purchases of geolocation data by the government.

Above all, the Fourth Amendment was forged to prevent general warrants.[226] The Star Chamber—the tyrannical British judicial body presided over by the King—weaponized general warrants not only against *known* "criti[cs] of the Crown."[227] General warrants allowed the government to rummage through people's personal papers and correspondence to unveil their political beliefs and rebellious activities, and persecute them on that basis.[228] Crucially, then, this device enabled the monarchy to discover *unknown* critics, dissenters, and rebels.

In the foundational English case *Entick v. Carrington*, counsel for plaintiff described the general warrant as a "monster of oppression" and so underscored the need to "tear into rags this remnant of Star Chamber tyranny."[229] The *Entick* Court ruled for the plaintiff, likening the general warrant to "so many Star Chamber decrees" that could not "be justified by the common law."[230] This rejection of the general warrant, then, represented a repudiation of the Star Chamber's method of uncovering unknown dissent, unorthodoxy, and private activity.

---

226. *See* Akhil Reed Amar, *Fourth Amendment First Principles*, 107 HARV. L. REV. 757, 786 (1994); 2 JOSEPH STORY, COMMENTARIES ON THE CONSTITUTION OF THE UNITED STATES § 1902 (Thomas M. Cooley ed., Boston: Little, Brown, and Co. 1873) (1825).

227. Walter B. Hamlin, *The Bill of Rights or the First Ten Amendments to the United States Constitution*, 68 COM. L.J. 233, 235 (1963).

228. *See* NELSON B. LASSON, THE HISTORY OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 45-49 (1937); *see also* Hamlin, *supra* note 227, at 234; Tracey Maclin, *supra* note 35, at 939-41.

229. 19 Howell's State Trials 1029 (1765).

230. *Id.*

The Supreme Court pronounced *Entick* as a guide to understanding what the Framers meant in framing the Fourth Amendment[231] and characterized the decision as when "individual liberty and privacy . . . finally won."[232] In *Keith*, the Supreme Court reiterated that "the fear of unauthorized official eavesdropping" must not "deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."[233] Under these circumstances, the Court stressed, "Fourth Amendment protections become [all] the more necessary."[234]

The Fourth Amendment was thus intended to make people's private political activities and individual lives illegible to the government (absent probable cause of criminal activity). In doing so, it prevented the possibility of government persecution for people's political beliefs, religious associations, and private activities.

Yet location data can reveal some of the most intimate details of people's lives. Location data can reveal whether someone is visiting an abortion clinic;[235] what faith they practice and how frequently they attend religious gatherings;[236] what their political associations and beliefs are;[237] what their immigration status is;[238] and much more.

---

231. *See* Boyd v. United States, 116 U.S. 616, 626-27 (1886) (explaining that the decision was "considered . . . as the true and ultimate expression of constitutional law" and "that its propositions were in the minds of those who framed the [F]ourth [A]mendment to the constitution"); *see also* NELSON B. LASSON, THE HISTORY AND DEVELOPMENT OF THE FOURTH AMENDMENT TO THE UNITED STATES CONSTITUTION 47-49 (1937).

232. Stanford v. Texas, 379 U.S. 476, 483 (1965).

233. United States v. U.S. Dist. Ct. for E. Dist. of Mich., S. Div., 407 U.S. 297, 314 (1972) (emphasis added).

234. *Id.*

235. *See* Cox, *Data Broker Is Selling Location Data*, *supra* note 4.

236. *See* Cox, *U.S. Military Buys Location Data*, *supra* note 39.

237. *See* Sam Schechner, Emily Glazer and Patience Haggin, *Political Campaigns Know Where You've Been. They're Tracking Your Phone*, WALL ST. J. (Oct. 10, 2019), https://www.wsj.com/articles/political-campaigns-track-cellphones-to-identify-and-target-individual-voters-11570718889 [https://perma.cc/HM5V-Y88W]; Charlie Warzel and Stuart A. Thompson, *How Your Phone Betrays Democracy*, N.Y. TIMES (Dec. 21, 2019), https://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html [https://perma.cc/MYL9-Q6V4].

238. *See* Lima, *supra* note 42.

Data brokers could sell extensive location records of people who visited abortion clinics to state governments that criminalize abortion.[239] National security agencies have already purchased location data from Muslim prayer and Muslim dating applications, each of which have tens of millions of users.[240] Immigration and Customs Enforcement purchased location data on individuals in sanctuary cities, even though those cities passed ordinances rejecting federal immigration detention requests.[241] And agencies may soon get into the business of purchasing other kinds of sensitive information like transaction and credit card histories.

The Fourth Amendment was forged to keep these kinds of information private to shield people from government persecution. This suggests a pressing need for *some* reform to protect against warrantless purchases of data. Yet, as the next section demonstrates, Fourth Amendment doctrine cannot supply the appropriate privacy protection.

B. Problems with Reinterpreting State Action

This Note established above that the key reason the Fourth Amendment does not regulate a government purchase of data is that purchases are not state action, nor does a purchase convert private actors into state actors. Because state action is the critical doctrinal pressure point, privacy proponents may believe that the best way to vindicate the purpose of the Fourth Amendment would be to creatively expand these stale concepts. Ultimately, though, the massive expansions in doctrine needed to regulate warrantless purchases are not only unlikely, but unattractive. This section will describe two potential expansions of Fourth Amendment doctrine that would expand state action to cover government purchases of data, and then describe the flaws and unintended consequences of both of these approaches.

---

239. *See* Cox, *Data Broker Is Selling Location Data*, *supra* note 4; Emma Bowman, *As States Ban Abortion, the Texas Bounty Law Offers a Way to Survive Legal Challenges*, NAT'L PUB. RADIO (July 11, 2022), https://www.npr.org/2022/07/11/1107741175/texas-abortion-bounty-law. [https://perma.cc/5M5J-427N]; Bobby Ally, *Privacy Advocates Fear Google Will Be Used to Prosecute Abortion Seekers*, NAT'L PUB. RADIO (July 11, 2022), https://www.wuft.org/nation-world/2022/07/11/privacy-advocates-fear-google-will-be-used-to-prosecute-abortion-seekers [https://perma.cc/C9H7-2XD9].

240. *See* Cox, *U.S. Military Buys Location Data*, *supra* note 39.

241. *See* Lima, *supra* note 42.

First, the public function doctrine could be expanded to include service providers' initial collection, at least when the information collected ends up in government hands. This would require lowering the bar from complete usurpation of a public function to partial fulfillment. Alternatively, inducement doctrine could be expanded to include economically induced sales of data packages. These broad doctrinal applications, however, risk creating enormous second-order effects.

Instead, Congress must step in to regulate sales of data. Congressional action presents several practical benefits that relying on the shifting sands of the Fourth Amendment preclude: mainly, that Congress can regulate more than just state actors. This Note thus underscores an urgent need for legislative action.

1. Expanding Public Function Doctrine: Monumental Collateral Consequences

Current public function doctrine recognizes that a private party can become a government actor when they completely usurp a public function exclusively reserved for the state. Even though they purchase user location data from brokers, law enforcement and intelligence agencies still seek warrants to obtain location data. While exact figures are not known, government purchases represent only a fraction of intelligence activities.[242] Thus, to extend the reach of the Fourth Amendment the bar must be lowered from usurpation to at the very least "partial fulfillment" of a public function. (This sets aside even the concern that surveillance is not "exclusively reserved" to the state.)

The unintended ramifications of such a doctrinal expansion are massive. Social media platforms, for example, have displaced town halls and other public forums as venues that host speech.[243] Twitter, Facebook, and every other social media app, then, would become government actors subject to the First Amendment. Content moderation that blocks offensive and harmful content may therefore become unconstitutional.[244] Beyond the

242. *See* Shenkman, *Legal Loopholes and Data for Dollars*, *supra* note 5.

243. *See Social Media Platforms and the Fight Against Election Disinformation*, NAT'L CONST. CTR. (Oct. 29, 2020), https://www.constitutioncenter.org/news-debate/americas-town-hall-programs/social-media-platforms-and-the-fight-against-election-disinformation [https://perma.cc/WW3T-B6SK].

244. *See* VALERIE C. BRANNON & WHITNEY K. NOVAK, CONG. RSCH. SERV., LSB10742, ONLINE CONTENT MODERATION AND GOVERNMENT COERCION (2022) ("Lower courts

monumental consequences on social media platforms, virtually any time the government enters into a contract with a private party to outsource its functions, those private parties would become government actors. When the government hires Boeing to construct new weapons systems, or a municipality hires a trash-collecting company to clean the streets, they would become state actors for constitutional purposes. In short, the risks of extreme overinclusion counsel against applying the public function doctrine in this way. But less expansive adjustments to the public function doctrine would fail to capture service providers under the Fourth Amendment.

2. Expanding Inducement Theory: Insufficient Reach

Expanding state action doctrine to cover a purchase of data, then, might be best accomplished through a creative application of inducement theory. However, suggesting that *any* open-market transaction with the government counts as economic inducement would similarly risk extreme overinclusion, as that would transform *every* actor that sells to the government into extensions of it (even if, for example, a contractor merely provides catering services to a military base). To limit second-order effects and remain faithful to the underlying rationale that animates the doctrine, economic inducement could be said to produce government action only where economic pressures render a transaction involuntary. Realistically, a transaction does not become involuntary solely as a result of market forces *most* of the time. But if there is any circumstance in which an open-market sale may not be voluntary due to purely economic factors, it is when the market is controlled by a single buyer.[245] If the government dominated the data market as a monopsonist or near-monopsonist buyer, brokers would *depend on the existence* of the government as a buyer. In that circumstance, there is good reason to believe that the prospect of a government purchase

have rejected [content moderation] claims, citing the well-established principle that private companies are not bound by the First Amendment's Free Speech Clause and therefore holding that the Constitution does not limit their ability to restrict user content.").

245. *See, e.g.*, Orley C. Ashenfelter, Henry Farber & Michael R. Ransom, *Labor Market Monopsony*, 28 J. LAB. ECON. 203 (2010) (describing how labor market monopsonists, i.e., employers, can set wages and prices that employees must accept); Kathryn Gary et al., *Monopsony Power and Wages: Evidence from the Introduction of Serfdom in Denmark*, 132 ECON. J. 2835, 2837 (2022) (finding that a monopsony in the labor market allowed employer to force lower wages on workers).

actually induces the brokers to sell user data and fully bend to the will of the government.[246]

This suggested amendment is doctrinally feasible. The idea that economic inducement cannot product inducement-as-state action derives largely from bounty hunting cases. Bounty systems have been upheld as legitimate largely because of the historic rule of *Taylor*: it is not state action because the relationship arises out of a *bounded contract* rather than legislative fiat.[247] Many commentators rightfully argue this doctrine is antiquated and that bounty hunters ought to be regarded as state actors precisely because of the inducement principle.[248] Such a proposal would also convert government contractors, such as builders of roads and defense contractors like Lockheed Martin and Northrop Grumman, into state actors; this, in turn, would require overturning *Rendell-Baker v. Kohn*.[249]

But problems exist with even this more limited proposal. Conceptually, if the new inducement principle is that "the government induces where it dominates the market," then all data brokers need to do to render the practice constitutional is to find other major buyers. This is a strange result.[250]

Pragmatically, even if this proposed doctrinal change was adopted, the current state of the world is a far cry from the circumstances under which the new inducement principle would kick in. As detailed above, data brokers do not just sell to law enforcement and intelligence agencies; large buyers include advertisers and other private actors in media, retail, and

246. *Id.*

247. *See* Taylor v. Taintor, 83 U.S. 366, 373-74 (1872).

248. *See, e.g.*, Jonathan Drimmer, *When Man Hunts Man: The Rights and Duties of Bounty Hunters in the American Criminal Justice System*, 33 HOUS. L. REV. 731, 739 (1996) (arguing that bounty hunters work extensively with the government, play a pivotal role, and should be considered state actors subject to constitutional restraints); Emily Michael Stout, *Bounty Hunters as Evidence Gatherers: Should They Be Considered State Actors Under the Fourth Amendment when Working with the Police?*, 65 U. CIN. L. REV. 665, 689 (1997) (arguing that bounty hunters should be subject to Fourth Amendment restrictions when working with police to apprehend fugitives).

249. 457 U.S. 830, 840-42 (1982).

250. This proposal also introduces extreme unpredictability. After all, how many sales of data to the government would put a data broker (or other government contractor) over the line? Determining the point at which a private actor becomes "induced" to sell their products is an empirical, economic question that Congress may be more apt to resolve.

healthcare.[251] Fourth Amendment protections would not follow until the government becomes a monopsonist or dominant buyer. Stretching inducement theory, therefore, either produces overbroad collateral effects but would subject data brokers to the Fourth Amendment, or limits second-order effects but would only apply in a hypothetical future scenario.

C. Reprogramming the Fourth Amendment—via Legislation

Given the difficulty of applying existing state action doctrine to regulate the purchase of data, Congress is better suited to resolve this vexing privacy puzzle via legislation. To accomplish this, Congress ought to pass comprehensive privacy legislation that both regulates the sale of sensitive data and bans foreign governments from buying these datasets. Such a law would address the privacy problem at its source, while mitigating a potentially grave foreign intelligence threat. This would require mixing elements of the proposed American Data Protection and Privacy Act with tight restrictions on sales to foreign governments.

A comprehensive privacy law of this kind is preferable to a sweeping ban on all government purchases, like FAINFSA—which was Congress's initial response to the privacy gap exposed by data brokers.[252] And, having passed the House Judiciary Committee,[253] it appears to be Congress's preferred mode of addressing the data broker problem. But passing this law would be the wrong way to protect privacy.

Admittedly, passing FAINFSA or a similar law would vindicate the promises of the Fourth Amendment. The Bill provides that a "law enforcement agency of a governmental entity and an element of the

251. *See Data Brokers Market Estimated to Reach US$ 462.4 billion by 2031*, TRANSPARENCY MARKET RSCH. (Aug. 1, 2022), www.globenewswire.com/news-release/2022/08/01/2489563/0/en/Data-Brokers-Market-Estimated-to-Reach-US-462-4-billion-by-2031-TMR-Report.html [https://perma.cc/9SK6-5U2U]; John Oliver, *Last Week Tonight: Data Brokers*, HOME BOX OFFICE (Apr. 11, 2022) [https://perma.cc/LHD6-4QTD].

252. *Coalition Calls for Congressional Hearings on the Fourth Amendment Is Not for Sale Act*, ACLU (Jan. 26, 2022), https://www.aclu.org/letter/coalition-calls-congressional-hearings-fourth-amendment-not-sale-act [https://perma.cc/5QR4-PG26].

253. *See* Warren Davidson, *Fourth Amendment Is Not for Sale Act Passes Judiciary Committee*, Warren Davidson Congressional Site (July 19, 2023) https://davidson.house.gov/2023/7/fourth-amendment-is-not-for-sale-act-passes-judiciary-committee [https://perma.cc/D5C7-TZ54].

intelligence community may not obtain from a third party in exchange for anything of value"[254] any "contents of communications" and "location information"[255] on any "covered persons."[256] Covered persons include people located in the United States and U.S. persons as defined by the Foreign Intelligence Surveillance Act, including citizens, aliens lawfully admitted for personal residence, and certain associations and corporations.[257]

Passing such a law might even present other benefits as well. Pushing for passage of the law might be more feasible than relying on creative applications of state action doctrine. Furthermore, codifying such a principle via doctrine runs the risk of allowing new factual development to change the privacy analysis. For example, the contractual terms of ToSs may begin to specify that data may be shared with government and may start to properly put users on notice. If a vendor begins selling people's data at a retail level, as one company did with ClearView AI, data purchases may suddenly become in "general public use," and disrupt users' reasonable expectation of privacy. Passing legislation presents the most promising way to plug this critical Fourth Amendment gap.

The principal problem with FAINFSA and similar legislation, then, is that it hobbles national security agencies relative to foreign threats. In the summer of 2023, the Office of the Director of National Intelligence confirmed in a declassified report that foreign governments *already* purchase Americans' data from third-party brokers.[258] Thus, these laws

254. Fourth Amendment Is Not for Sale Act, H.R. 2738, 117th Cong. § 2703(e)(2)(A) (2021).

255. *Id.* § 2702(e)(1)(c)(ii)

256. *Id.* § 2703(e)(1)(B)

257. *Id.* FISA defines USPs as follows: "United States person" means a citizen of the United States, an alien lawfully admitted for permanent residence (as defined in section 1101(a)(20) of title 8), an unincorporated association a substantial number of members of which are citizens of the United States or aliens lawfully admitted for permanent residence, or a corporation which is incorporated in the United States, but does not include a corporation or an association which is a foreign power, as defined in subsection (a)(1), (2), or (3). 8 U.S.C. § 1801(i).

258. *See* Office of the Director of National Intelligence Senior Advisory Group, *Report to the Director of National Intelligence* 3 (June 9, 2023), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [https://perma.cc/9U9P-8QU3]; Austin Williams, *Report: Data Brokers Selling Personal Information to*

would only prohibit warrantless purchases of data by the U.S. government, but under FAINFSA (or the Fourth Amendment), brokers would still be free to sell sensitive geolocation data to hostile foreign threats and governments *without restraint*. The Framers never could have envisioned a world where private actors would have better surveillance capabilities than the government, let alone be able to sell that information to hostile foreign threats.

In light of this problem, some may believe the appropriate solution is to shore-up the wall between intelligence and law enforcement agencies, imposing tighter collection rules on the latter but permitting laxer restrictions on the former; after all, it is law enforcement agencies that have the power to enact violence on individuals by sending them to prison and prosecuting them.

Rather than regulate a downstream effect, however, Congress should address the source of this problem: that these invasive kinds of data are transacted on the market in the first place. This key vulnerability thus counsels in favor of regulating data sales by private actors, whoever the buyer happens to be.

Indeed, appetite for this kind of solution has been aptly demonstrated on the Hill. A similar but less direct foreign intelligence threat vulnerability prompted a bipartisan coalition of Senators (Wyden, Whitehouse, Rubio, Lummis, and Hagerty) and Representatives (Eshoo and Davidson) to propose the Protecting Americans' Data From Foreign Surveillance Act (PADFFSA) in summer 2022, largely in response to the surge in popularity of TikTok.[259] Senator Wyden alerted his fellow legislators to the fact that "[r]ight now it's perfectly legal for a company in China to buy huge databases of sensitive information from data brokers about the movements or health records of millions of Americans, and then share that information with the Chinese government."[260] Senator Lummis similarly offered that

US Government, Private Entities, Foreign Governments, FOX 5 (June 15, 2023), https://www.fox5ny.com/news/report-data-brokers-selling-personal-information-to-us-government-private-entities-foreign-governments [https://perma.cc/J226-6MZL].

259. *See* Protecting Americans' Data from Foreign Surveillance Act of 2022, S. 4495, 117th Cong.; Protecting Americans' Data From Foreign Surveillance Act of 2023, H.R. 4108, 118th Cong.

260. Press Release, Office of Ron Wyden, United States Senator for Oregon, *Wyden, Lummis, Whitehouse, Rubio, and Hagerty Introduce Bipartisan Legislation to Protect Americans' Private Data from Hostile Foreign Governments* (June 23, 2022), https://www.wyden.senate.gov/news/press-releases/wyden-

"[a]llowing foreign adversaries unrestricted access to Americans' private, sensitive data . . . threatens our national security."[261] Representative Eshoo, too, lamented that "there are no laws preventing foreign companies from purchasing and sharing large quantities of Americans' personal data."[262] Senators Rubio, Hagerty, and Whitehouse expressed similar sentiments. But this law sought to regulate purchases by foreign *companies* via reforms to export control laws as regulated by the Commerce Department. Even more direct than TikTok and foreign company purchases, foreign intelligence apparatuses are free to buy data directly from third-party brokers. Rather than create a patchwork of regulation by restricting categories of buyers, Congress ought to regulate this problem at the source: the seller. Indeed, several states have recently passed laws requiring data brokers to register and report on their activities concerning citizens (though have declined to adopt more extensive regulatory restrictions).[263]

This Note therefore advances a mix of two different proposed laws to tackle this privacy problem: PADFFSA and the American Data Protection and Privacy Act (ADPPA). The ADPPA element would address the fundamental privacy problem by regulating sales of sensitive data, regardless of buyer. ADPPA would create a "third party registry," much like California's data broker registry. In addition to meeting reporting requirements, these third parties would only be permitted to transfer people's data if they first obtained the "affirmative express consent of the individual."[264] This would require the data transferor (e.g., a broker) to make a "specific request" to the individual, make a "clear and conspicuous standalone disclosure," and identify with particularity the data the third party seeks to transfer.[265] Absent this, data can only be transferred when

lummis-whitehouse-rubio-and-hagerty-introduce-bipartisan-legislation-to-protect-americans-private-data-from-hostile-foreign-governments [https://perma.cc/7YWP-AV8Q].

261. *Id.*

262. Press Release, Office of Warren Davidson, United States Representative for Ohio's Eighth District, *Reps. Davidson, Eshoo Introduce the Protecting Americans' Data from Foreign Surveillance Act* (June 14, 2023), https://davidson.house.gov/2023/6/reps-davidson-eshoo-introduce-the-protecting-americans-data-from-foreign-surveillance-act [https://perma.cc/B7RY-HFR4].

263. *See* Cal. Civ. Code § 1798.99.80; Texas S.B. 88-2105; 9 V.S.A. §§ 2446, 2447.

264. American Data Protection and Privacy Act (ADPAA) H.R. 8152, 117th Cong. § 102(A) (2022).

265. *Id.* § 2(1)(A), (B)(i)-(ii)

"necessary to comply with a legal obligation imposed by . . . law," to "prevent an individual from imminent injury," or "at the direction of a government entity" insofar as it is authorized by law, or to "establish, exercise, or defend legal claims."[266] Notably, these match the "legal bases" under which the data may permissibly be processed under the GDPR.[267] ADPPA, however, "does not permit . . . the transfer of covered data for payment or other valuable consideration to a government entity."[268] And like the California Consumer Protection Act and the GDPR, users would have the right to delete personal information collected on them, the right to know about the records collected on them, and the right to opt out of data sales—rights that can be enforced on the Federal Trade Commission (FTC) website.[269] To foster compliance, the FTC would have the power to bring enforcement actions and levy hefty fines. Individuals and states would have the right to bring suit as well. The FTC, furthermore, would have rulemaking authority power to define new categories of sensitive data subject to these restrictions.

The provisions of the ADPPA present effective solutions to the privacy puzzle posed by data sales. By limiting most transactions to those which users have unambiguously consented and providing for rights to opt-out, users can finally feel secure that their information is private from not only the government, but from everyone. Granting an agency rulemaking authority to define new categories of sensitive data is sensible too, vindicating the mosaic theory of the Fourth Amendment: categories of data that once may not have been invasive can, when put in conversation with other data, become deeply revealing. It makes sense to allow an agency to update the kinds of data that qualify as sensitive. Finally, as the fines issued under the GDPR aptly demonstrate, granting the relevant agency the power to bring enforcement actions is an effective method of enforcing data privacy.

Regulating sales under the provisions of ADPPA alone, however, does not address the foreign intelligence threat discussed above. ADPPA permits transfers of sensitive data to government entities, but only insofar as it is legally authorized—and would not permit the government to purchase the data as an end-run around warrants. Theoretically, registered brokers could sell the data of consenting Americans to foreign corporations, governments, and instrumentalities.

---

266. *Id.* § 102(3).

267. General Data Protection Regulation, Art. 6(1)(a)-(f).

268. ADPPA § 102(3).

269. *Id.* § 206(b)(3)(c)(i) ("Do Not Collect" provision); *Id.* § 204(b)(1) (opt-out provision).

That is why new comprehensive legislation should combine the ADPPA with elements of PADFFSA. This would manage the foreign intelligence threat by enacting even tighter restrictions on sales to foreign entities. PADFFSA, a proposed amendment to the Export Control Reform Act, would empower the Secretary of Commerce to control the export of personal data—i.e., data sales to foreign entities. The Secretary, in coordination with other elements of the U.S. government, would identify categories of sensitive data that could either (A) "be exploited by foreign governments or foreign adversaries," and (B) "harm the national security of the United States" if sold in a large enough quantity (which is a threshold to be determined by the Secretary).[270] Through administrative rulemaking, the Secretary would identify data falling in each category, and would determine the threshold that would apply to data under category (B). These kinds of data would be subject to exports control procedures, and generally require a license or specific authorization to proceed with the data sale.[271]

Comprehensive data privacy legislation should stitch together these two laws. This would address the privacy gap posed by data sales at the foundation, while not putting U.S. intelligence agencies at a tactical disadvantage relative to foreign entities. Granted, this Frankenstein legislation would require consolidating the parallel procedures established in these two laws. Most notably, ADPPA would grant the FTC rulemaking power to define categories of sensitive data, while PADFFSA would give the Secretary of Commerce this authority. Comprehensive privacy legislation would streamline these parallel processes by empowering one data protection authority to define the categories of sensitive data, while allowing the FTC to bring enforcement actions against U.S.-based data brokers (and other sellers of sensitive data) and the Commerce Department to restrict data sales to foreign companies. This Note does not take a position on where this authority ought to be seated. But this cohesive approach to protecting privacy is superior to FAINFSA's.

Congress, unhindered by the state action constraints inherent in the Fourth Amendment, is free to regulate not just *government* purchases of data, but the original sales of sensitive data. Indeed, the General Data

270. Protecting American' Data From Foreign Surveillance Act of 2023, S. 1974, 118th Cong. § 1758A(1)(A)-(B).

271. *Id.* § 1758A(b)(2)(A)(i).

Protection Regulation (GDPR)[272] and the American legislation it inspired[273] opt to regulate the private sector rather than the public sector. This presents Congress with a profound opportunity to restore the principles that animate the Fourth Amendment and keep people's personal lives truly secure—not just against state and federal government, but against everyone.

CONCLUSION

The data brokering market denotes a serious loophole in privacy protections, but it is emblematic of a wider, systemic issue. Despite some strides in *Carpenter*, Fourth Amendment doctrine has repeatedly demonstrated itself unfit to keep pace with the novel privacy issues that attend evolving surveillance technology. Brokers are thus just one speck in a wider constellation of emerging privacy challenges raised by new surveillance methods. Short of doctrinal overhaul, contorting constitutional law is unlikely to transform the Fourth Amendment into the anti-persecution bulwark that it was meant to be. The Constitution's inability to address these privacy issues alone underscores an urgent need for Congress to forge a regulatory scheme to keep up with emerging issues that attend novel surveillance practices. Otherwise, people may become victim to electronic general warrants.

272. GDPR data privacy regulations do not apply to government bodies and law enforcement agencies when data is gathered and processed to prevent, investigate, detect, or prosecute criminal offenses.

273. This includes the California Consumer Privacy Act, the proposed American Data Protection and Privacy Act, and the New York Privacy Law.