GOVERNMENT PURCHASES OF PRIVATE DATA

Matthew Tokson[*]

In recent years, numerous government entities, from the Department of Homeland Security to local police departments, have begun to purchase location and other data from specialized brokers to track individuals' activities over time. Much of this data is constitutionally protected. Yet, while some government actors have concluded that the Fourth Amendment regulates these purchases, most have determined that purchasing data is a valid way of bypassing the Constitution's restrictions.

This Article addresses the increasingly prominent issue of government purchases of private data and examines broader issues of privacy protection in an era of commercial markets in personal information. The Article questions the widespread assumption that the Fourth Amendment can never apply to commercial purchases. Police officers can generally purchase an item available to the public without constitutional restriction. But a closer examination of data markets demonstrates that sensitive cellphone data is not publicly available or exposed. Rather, the vendors who sell such data do so either exclusively to law enforcement agencies or in large, anonymized chunks to other marketing companies. Because sensitive cellphone data remains functionally private, a government purchase of such data violates the Fourth Amendment.

The Article then challenges the idea that consumers waive their rights to their cellphone data when they use apps or other services. The explanations customers see when an app asks for permission to access their data are often insufficient or misleading, and they typically say nothing about personal data being sold to other parties. Further, penalizing users for disclosing their data to service providers

* Professor, University of Utah S.J. Quinney College of Law. Thanks to Hannah Bloch-Wehba, Alicia Boyd, Ryan Calo, Danielle Citron, Barry Friedman, Orin Kerr, Paul Ohm, Natalie Ram, Victoria Schwartz, Chris Sohogian, Angela Turnbow, Wayne Unger, and all participants at the Privacy Law Scholars Conference. Special thanks to Chelsea Smith for excellent research assistance.

creates harmful incentives and is incompatible with meaningful Fourth Amendment protection in the digital age.

The Article sits at the intersection of consumer privacy and Fourth Amendment law, as poorly regulated markets in personal data and flawed concepts of consumer consent now threaten to erode fundamental constitutional rights. The Article draws broader lessons about the inadequacy of consumer privacy law in the United States. It examines the potential for private surveillance to become government surveillance via technical and legal interoperability. And it assesses a variety of possible solutions through which legal actors can prevent commercial markets in private data from undermining Fourth Amendment rights.

TABLE OF CONTENTS

INTRODUCTION 270
I. BACKGROUND AND CONTEXT 279
A. Third-Party Data 279
B. Location Data 281
C. The Government in Data Markets 283
II. GOVERNMENT PURCHASES AND FOURTH AMENDMENT LAW .. 288
A. Limited Commercial Availability 288
B. The General Public Use Standard 293
C. Government Purchases and Anti-Evasion Principles 296
1. Co-Tenants and Retail Stores 298
2. A Case Study 300
III. DATA COLLECTION AND CONSENT 301
A. The Meaninglessness of App Permissions 303
B. Automatic Disclosure 307
C. Inescapability 308
D. Additional Carpenter Factors 310
IV. IMPLICATIONS AND SOLUTIONS 312
A. The Inadequacy of Consumer Privacy Law 312
B. Surveillance Interoperability 314
C. Potential Solutions 316
1. Jurisprudential 316
2. Statutory 319
3. Regulatory 321
CONCLUSION 323

INTRODUCTION

In 2018, U.S. Immigration and Customs Enforcement ("ICE") began purchasing access to cellphone users' digital location data

through a data brokerage company called Venntel.[1] The data had been collected from popular cellphone apps, including weather, shopping, and video game apps.[2] ICE used Venntel's service to track the movements of cellphone users in areas near the United States' southern border.[3] At one point, ICE discovered that cellphones were moving back and forth across the border in what was likely an underground smuggling tunnel that terminated in a closed Kentucky Fried Chicken ("KFC") restaurant in San Luis, Arizona.[4] ICE passed this information to the local police department, which made an apparently pretextual traffic stop of Ivan Lopez, the KFC's owner, and found large quantities of drugs.[5] ICE officers then obtained a search warrant for the KFC and found the tunnel they already knew was there.[6] The San Luis police kept any mention of the cellphone tracking out of their records and initially attributed their traffic stop of Lopez to an "equipment violation."[7]

Of course, not every law enforcement use of location tracking services detects a criminal. In 2018, the Missouri State Highway Patrol ("MSHP") began purchasing a location-tracking service known as Fog Reveal, which enabled them to track cellphone users via app-collected location data.[8] They used it while investigating the murder of Ben Renick, an exotic snake breeder found lying in a pool of his own

---

1. Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020, 7:30 AM), http://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600.

2. *Id.*

3. *Id.*

4. *Id.*; *see also Drug Tunnel Ran from Old KFC in Arizona to Mexico Bedroom*, BBCNEWS (Aug. 23, 2018), http://www.bbc.com/news/world-us-canada-45291978.

5. *See* Tau & Hackman, *supra* note 1.

6. *See* Amy B. Wang, *Drug-Smuggling Tunnel to Mexico Found Under Abandoned KFC in Arizona*, WASH. POST (Aug. 24, 2018, 5:29 PM), http://www.washingtonpost.com/nation/2018/08/24/drug-smuggling-tunnel-mexico-found-under-abandoned-kfc-arizona (noting that ICE officials, not local police, searched the KFC).

7. *See* Tau & Hackman, *supra* note 1; Matthew Martinez, *Vacant KFC Became One End of a Drug Tunnel to Mexico. Video Shows Extensive Design*, FORT WORTH STAR-TELEGRAM (Aug. 23, 2018, 8:46 AM), http://www.star-telegram.com/news/nation-world/national/article217188080.html.

8. Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget*,*'* APNEWS (Sept. 2, 2022, 5:28 PM), http://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef; Bennett Cyphers, *How Law Enforcement Around the Country Buys Cellphone Location Data Wholesale*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), http://www.eff.org/deeplinks/2022/08/how-law-enforcement-around-country-buys-cell-phone-location-data-wholesale.

blood at his breeding facility.[9] The MSHP used Fog Reveal to search for cellphones at the facility and in Renick's home, and they zeroed in on a particular mobile device.[10] Working closely with a Fog Reveal employee, the MSHP tracked this cellphone user, obtaining a "pattern of life" analysis by tracking everywhere the person went for the previous month, likely capturing hundreds of location data points every day.[11] The person whose life was patterned in such detail turned out to be the Renicks' babysitter, who was not involved in the murder.[12]

Personalized location tracking is a powerful tool of government surveillance. Its use without a warrant was thought to be unlawful following the Supreme Court's landmark ruling against warrantless cellphone tracking in 2018's *Carpenter v. United States*.[13] But in recent years, numerous federal, state, and local government entities have purchased location tracking services for law enforcement and other purposes.[14] Government attorneys and observers have concluded that such purchases allow police to collect otherwise protected data without violating the Constitution.[15]

---

9. Burke & Dearen, *supra* note 8; *see also* Lauren Turner Dunn, *Ben Renick Case: A Look at the Murder of the World-Renowned Snake Breeder*, CBS NEWS (Mar. 11, 2022, 1:40 AM), http://www.cbsnews.com/news/ben-renick-snake-breeder-murder-timeline.

10. Burke & Dearen, *supra* note 8.

11. *See* Cyphers, *supra* note 8 (describing the Renick investigation and noting that, in a similar investigation, the MSHP obtained an average of 263 location data points per day, almost one every five minutes).

12. Renick's wife Lynlee and her boyfriend eventually admitted to the killing, although each claimed that the other had shot Renick. *E.g.*, Jeff Truesdell, *A Reptile Breeder Was Killed by One of His Snakes, the 911 Caller Said. Then Bullet Wounds Were Found*, PEOPLE (Oct. 5, 2022, 10:00 AM), http://people.com/crime/ben-renick-murder-wife-lynlee-convicted. Police were tipped off after another of Lynlee's boyfriends told police that she'd admitted murdering her former husband. *See* Charles Dunlap, *A Montgomery County Man with a $1 Million Snake-Breeding Operation Was Killed in 2017. His Wife's Murder Trial Starts Monday*, COLUMBIA DAILY TRIB. (Dec. 5, 2021, 6:45 AM), http://www.columbiatribune.com/story/news/courts/2021/12/05/murder-trial-for-wife-of-montgomery-county-missouri-snake-breeder-ben-renick-set-to-begin/8838919002.

13. 138 S. Ct. 2206, 2223 (2018).

14. *See infra* Subpart I.C.

15. *See, e.g.*, Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 25, 2021), http://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html (reporting that the Defense Intelligence Agency does not believe that the Fourth Amendment requires a warrant for the purchase or use of commercially available data); Tau & Hackman, *supra* note 1 (reporting that government lawyers have concluded that the Fourth Amendment does not apply to location data because it can be purchased); *see also* Orin S. Kerr, *Buying Data and the Fourth Amendment*, *in* HOOVER INSTITUTION AEGIS PAPER SERIES 1, 1 (Nov. 17, 2021),

Far from being limited to location information, this principle can easily encompass other forms of data collected by cellphone apps and internet services—web-surfing data, contact lists, dating profiles, search terms, user profiles, health data, and more.[16] In recent years, government agencies have expanded their purchases of such data, buying web-surfing records and other sensitive digital data on the activities of hundreds of millions of Americans.[17] A recent report from the United States Office of the Director of National Intelligence found that today, commercially available information "'includes information on nearly everyone that is of a type and level of sensitivity that historically could have been obtained' through targeted collection methods such as wiretaps, cyber espionage, or physical surveillance."[18]

This issue is increasingly central to digital privacy in the modern era. Location, web-surfing, and other digital data can be extremely revealing of the details of our personal lives. Such data provides a detailed record of an individual's movements and activities.[19] It can reveal their familial, political, professional, religious, and sexual associations.[20] Permitting the government to purchase sensitive digital information without constitutional restraint raises the prospect of panoptic government observation of people's lives. With

---

http://www.hoover.org/research/buying-data-and-fourth-amendment (contending that the Fourth Amendment does not apply to government purchases, at least under current circumstances). *But see* Byron Tau, *Treasury Watchdog Warns of Government's Use of Cellphone Data Without Warrants*, WALL ST. J. (Feb. 22, 2021, 9:24 AM), http://www.wsj.com/articles/treasury-watchdog-warns-of-governments-use-of-cellphone-data-without-warrants-11614003868 (describing a Treasury Department report casting doubt on the legality of IRS purchases of private location data).

16. *See infra* notes 320–37 and accompanying text.

17. *See, e.g.*, Joseph Menn, *Senator Seeks FTC Probe of Data Sales to U.S. Government Agencies*, WASH. POST (Dec. 15, 2022, 10:00 AM), http://www.washingtonpost.com/technology/2022/12/15/wyden-ftc-neustar-sussmann; Dell Cameron & Mack DeGeurin, *Whistleblower: Pentagon Purchased Mass Surveillance Tool Collecting Americans' Web Browsing Data*, GIZMODO (Sept. 21, 2022), http://gizmodo.com/ncis-whistleblower-military-data-broker-cymru-wyden-1849564984; Letter from Ron Wyden, U.S. Sen., & Cynthia M. Lummis, U.S. Sen., to Merrick Garland, Att'y Gen. (Mar. 29, 2023), http://s3.documentcloud.org/documents/23729538/wyden-letter-sources.pdf.

18. Byron Tau & Dustin Volz, *U.S. Spy Agencies Buy Vast Quantities of Americans' Personal Data, U.S. Says*, WALL ST. J. (June 12, 2023, 2:28 PM), http://www.wsj.com/articles/u-s-spy-agencies-buy-vast-quantities-of-americans-personal-data-report-says-f47ec3ad (quoting OFF. OF THE DIR. OF NAT'L INTEL. SENIOR ADVISORY GRP. PANEL ON COMMERCIALLY AVAILABLE INFO., REPORT TO THE DIRECTOR OF NATIONAL INTELLIGENCE 2–3 (Jan. 27, 2022), http://www.odni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf).

19. *See* Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

20. *Id.*

this awesome power comes the potential for abuse; police abuses of data surveillance for personal and political purposes have already begun to come to light.[21] More instances of abuse are likely to arise as the practice of surveillance via purchased data continues to spread.

This Article addresses the important and novel issue of government purchases of private data and examines the broader issue of privacy protections in an era of markets in personal information. It raises concerns about the ability of the government to surveil virtually any citizen in remarkable detail via their cellphone data. And it questions the widespread assumption that the Fourth Amendment can never apply to commercial purchases.

Police officers can generally purchase items available to the public without constitutional restriction.[22] But this Article's detailed examination of data markets reveals that this sensitive data is not commercially available to the general public. Rather, it is available only to government agencies, or in large, anonymized blocks of data processed by corporate entities and inaccessible to the public.[23] The specialized contractors that sell location tracking services and related data to law enforcement typically sell to the government exclusively.[24] These companies often go to extreme lengths to avoid disclosing *any* information about their services to the public.[25] And the cost of these services, ranging from several thousands to hundreds of thousands of dollars per year, would be prohibitively high for most consumers.[26] Likewise, data sold commercially to facilitate targeted advertising is sold to marketers and ad companies in large, anonymized blocks of

21. *See, e.g.*, Yan Fang, *The Managerialization of Search Law and Procedure for Internet Evidence* (manuscript on file with author) (describing abusive police uses of geofence warrants for political and personal purposes); Charlie Warzel & Stuart A. Thompson, *How Your Phone Betrays Democracy*, N.Y. TIMES (Dec. 21, 2019), http://www.nytimes.com/interactive/2019/12/21/opinion/location-data-democracy-protests.html (describing governments' use of location data to track and punish protesters); Rehberg v. Paulk, 611 F.3d 828, 835 (11th Cir. 2010) (recounting a district attorney's abusive use of subpoena power to investigate a critic of his political allies).

22. *See* Maryland v. Macon, 472 U.S. 463, 469–70 (1985).

23. *See infra* Subpart II.A.

24. *See infra* notes 136–64 and accompanying text.

25. *See* Tau & Hackman, *supra* note 1; Martinez *supra* note 7; *infra* notes 139–46 and accompanying text.

26. *See* Tau & Hackman, *supra* note 1; Burke & Dearen, *supra* note 8.

data.[27] It is not designed or processed for individualized tracking and is unavailable to the general public.[28]

The Article then turns to the legal context of limited commercial markets in private data. It finds that, even if a court were to deem location and other sensitive data commercially available to the public, it would remain protected by the Fourth Amendment. An underappreciated line of Fourth Amendment precedents bars police officers from intrusive activities that private citizens could, in theory, undertake but generally do not.[29] Purchases of sensitive data collected by cellphone apps fit this framework—even if such data is available to some commercial entities, it is not publicly exposed in any meaningful way. When the government obtains such private data without a warrant, by purchase or other means, it violates the Fourth Amendment.[30]

As this Article demonstrates, there is nothing special about a commercial transaction that allows it to strip otherwise protected data of its constitutional protections or to immunize otherwise unlawful government acts. The government could not, for example, pay a contractor to take infrared photographs revealing the inside of a person's house without violating the Fourth Amendment.[31] Such a contractor would likely be considered a state actor, and in any event, the government would violate the homeowner's reasonable expectation of privacy in their home.[32] Moreover, longstanding "anti-evasion" principles in constitutional law provide that government actors cannot circumvent constitutional restrictions via workarounds or technicalities, including employing private actors to perform a public function.[33] The fact that the government obtained information

---

27. 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), http://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html; Matthew Tokson, *Automation and the Fourth Amendment*, 96 IOWA L. REV. 581, 603, 607 (2011).

28. *See infra* notes 152–64 and accompanying text. In addition, aggregated location data processed for commercial purposes is sometimes prohibitively difficult to deanonymize, even for determined experts. *See* Valentino-DeVries et al., *supra* note 27.

29. *See* Florida v. Jardines, 569 U.S. 1, 9, 11 (2013); Kyllo v. United States, 533 U.S. 27, 34, 39 n.6 (2001); Bond v. United States, 529 U.S. 334, 338–39 (2000).

30. *See infra* Subpart II.B.

31. *See infra* notes 188–98 and accompanying text.

32. *See infra* notes 189–91 and accompanying text.

33. Brannon P. Denning & Michael B. Kent, Jr., *Anti-Evasion Doctrines in Constitutional Law*, 2012 UTAH L. REV. 1773, 1776–77 (2012); *see, e.g.*, Lingle v. Chevron U.S.A., Inc., 544 U.S. 528, 539 (2005) (noting that the Takings Clause addresses both traditional takings and their functional equivalents); Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 298 (2001) (treating private actors pervasively entwined with public officials and institutions as public actors); Best & Co. v. Maxwell, 311 U.S. 454, 456–57 (1940) (holding that

via a commercial transaction is insufficient to immunize its actions against constitutional scrutiny.

The Article then challenges the idea that consumers consent to the government collecting and tracking their cellphone data when they disclose such data to apps and other service providers.[34] While consumers often give permission to apps to collect and use their data, these agreements do not dictate the scope of Fourth Amendment consent.[35] Further, the explanations customers see when an app asks for permission to access their data are often incomplete or misleading, and they typically say nothing about personal data being sold or shared with other parties.[36] Most users struggle to fully understand the complex commercial and technological infrastructures underlying their cellphone apps.[37] Neither can customers be reasonably expected

---

the Constitution prohibits state laws that discriminate against interstate commerce even if they are crafted to be facially neutral); Lane v. Wilson, 307 U.S. 268, 275 (1939) (holding that the Fifteenth Amendment bars government actions that practically restrict voting based on race even if they do not facially discriminate based on race); Byars v. United States, 273 U.S. 28, 32 (1927) ("[T]he court must be vigilant to scrutinize the attendant facts with an eye to detect and a hand to prevent violations of the Constitution by circuitous and indirect methods."); Cummings v. Missouri, 71 U.S. 277, 325 (1866) ("If the [Bill of Attainder Clause] can be evaded by the form of the enactment, its insertion in the fundamental law was a vain and futile proceeding.").

34. Government attorneys have made this argument to help justify government purchases of personal data. *See* Tau, *supra* note 15 (reporting that many government lawyers have concluded that *Carpenter* does not apply to app data); Letter from J. Russell George, Inspector Gen. for Tax Admin., Dep't of the Treasury, to Ron Wyden, U.S. Sen., & Elizabeth Warren, U.S. Sen. (Feb. 18, 2021), http://s.wsj.net/public/resources/documents/Response.pdf [hereinafter Treasury Letter] (describing IRS officials' conclusion that app data is voluntarily disclosed and therefore unprotected under *Carpenter*).

35. Contractual rights and Fourth Amendment rights are not coextensive, especially for contracts between two private parties. *See, e.g.*, Byrd v. United States, 138 S. Ct. 1518, 1529 (2018) (concluding that a breach of a rental contract has no bearing on an individual's Fourth Amendment rights); Carpenter v. United States, 138 S. Ct. 2206, 2235–36 (2018) (Thomas, J., dissenting) (noting that the majority opinion protects the defendant's interest in his cell phone location data records despite his lack of any contractual right in the records); United States v. Washington, 573 F.3d 279, 284–85 (6th Cir. 2009) (holding that a violation of lease terms did not affect a tenant's Fourth Amendment rights); United States v. Cunag, 386 F.3d 888, 895 (9th Cir. 2004) (noting that obtaining a hotel room by fraud in violation of the rental agreement did not eliminate the occupant's Fourth Amendment rights in his hotel room); Orin S. Kerr, *Terms of Service and Fourth Amendment Rights*, U. PA. L. REV. (forthcoming 2023) (contending that terms of service are irrelevant to Fourth Amendment rights).

36. *See infra* notes 245–49 and accompanying text.

37. *See* Neil Richards & Woodrow Hartzog, *The Pathologies of Digital Consent*, 96 WASH. U. L. REV. 1461, 1478–79 (2019); Daniel Solove, *Introduction: Privacy Self-Management and the Consent Dilemma*, 126 HARV. L. REV. 1880, 1883–86 (2013). In reality, users are prone to blindly grant permissions to their

to read or comprehend the detailed privacy policies of every app or service they encounter.[38]

In addition, much of the personal data collected by cellphone apps is not voluntarily disclosed to the apps at all. Cellphone data collection is frequently automatic, occurring without any affirmative act by the user.[39] Moreover, the use of cellphone apps is extremely widespread and virtually inescapable for most Americans.[40] And while consumers can theoretically opt out of disclosing data to such apps, in practice, denying apps permission to access user data often renders them largely useless.[41] Accordingly, consumers frequently have little choice but to disclose their cellphone data. This data is often deeply revealing of its users' private lives and collected in large quantities.[42] Under the Supreme Court's most recent Fourth Amendment precedents, data that is deeply revealing, voluminous, and not voluntarily disclosed to others remains protected by the Fourth Amendment.[43]

More generally, penalizing users for disclosing their data to service providers creates harmful incentives and is incompatible with meaningful Fourth Amendment protection in the digital age. It would also create substantial inequalities in Fourth Amendment law. Technologies that are optional for most people are often unavoidable

---

cellphone apps, especially when confronted with numerous permission requests during the initial set-up of their cellphones. *See* Marc Chase McAllister, *Modernizing the Video Privacy Protection Act*, 25 GEO. MASON L. REV. 102, 110 (2017); *Why Do We Blindly Sign Terms of Service Agreements?*, NPR (Sept. 1, 2014) [hereinafter NPR], http://www.npr.org/2014/09/01/345044359/why-do-we-blindly-sign-terms-of-service-agreements.

38. *See infra* notes 257–62 and accompanying text. Each user would also have to dedicate hundreds of hours of their lives each year to read all of the privacy policies that apply to them in the digital era. *See* Aleecia M. McDonald & Lorrie Faith Cranor, *The Cost of Reading Privacy Policies*, 4 I/S: J.L. & POL'Y FOR INFO. SOC'Y 543, 564–65 (2008).

39. *See infra* Subpart III.B.

40. *See infra* Subpart III.C.

41. *See, e.g.*, McAllister, *supra* note 37, at 110.

42. *See infra* Subpart III.D.

43. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); Matthew Tokson, *The Aftermath of* Carpenter*: An Empirical Study of Fourth Amendment Law, 2018–2021*, 135 HARV. L. REV. 1790, 1795, 1822 (2022); *see also* Riley v. California, 573 U.S. 373, 393–94, 403 (2014) (holding that police could not search cellphones incident to arrest in part because cellphones contain revealing information and have immense storage capacity); United States v. Jones, 565 U.S. 400, 430–31 (2012) (Alito, J., concurring in the judgment) (contending that tracking a car via a GPS signal for an extended period violated the Fourth Amendment, in an opinion joined by three other Justices and endorsed by a fourth).

for others, including people with disabilities, people in poverty, and other disadvantaged populations.[44]

The Article draws broader lessons about the inadequacy of consumer privacy law in the United States. The lack of a comprehensive privacy statute, poorly regulated domestic markets in personal data, and the flawed concepts of consumer consent that underlie lawmakers' indifference towards these issues now threaten to erode fundamental Fourth Amendment rights. The "notice and choice" approach currently dominant in United States law allows companies to use consumer data for virtually any purpose so long as they disclose those uses in a privacy policy or terms of use document.[45] This gives rise to barely regulated markets in personal data used for marketing and algorithmic decision-making purposes.[46] Lawmakers' failure to effectively oversee these markets gives rise to the law enforcement practices that currently undermine constitutional protections.

In this context, private and government surveillance are interoperable. That is, technologies of private monitoring can easily be leveraged by government actors to monitor individuals.[47] Not only can the government track the locations of its citizens, but it can analyze web-surfing data to keep track of protest movements,[48] or use health and menstruation tracking apps to enforce abortion laws or discriminatory laws against transgender persons.[49] Private surveillance is innately compatible with law enforcement surveillance via markets in individualized tracking and profiling.[50]

Finally, the Article assesses potential solutions through which legal actors can prevent commercial data markets from undermining Fourth Amendment rights. Courts could require warrants for government purchases of private data, although government efforts to obscure sources of information and keep evidence of purchases out of court will likely make this difficult. Surveillance targets may have to obtain data about government purchases via the federal Freedom of Information Act ("FOIA") or other transparency laws.[51] Legislatures could address government purchases of data either

---

44. *See* Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409, 409 (2021).

45. *See, e.g.*, Neil Richards & Woodrow Hartzog, *Taking Trust Seriously in Privacy Law*, 19 STAN. TECH. L. REV. 431, 444 (2016).

46. *See infra* Subpart IV.A.

47. *See infra* Subpart IV.B.

48. *See, e.g.*, Warzel & Thompson, *supra* note 21; Daniel Politi, *USA Today Fights FBI Effort to Obtain IP Addresses of People Who Read an Article*, SLATE (June 5, 2021, 12:52 PM), http://slate.com/news-and-politics/2021/06/usa-today-fbi-subpoena-ip-addresses-article.html.

49. *See infra* notes 331–37 and accompanying text.

50. *See infra* Subpart IV.B.

51. *See infra* Subpart IV.C.1.

through narrow legislation or broader statutes regulating consumer privacy. The successes and failures of Europe's approach to data regulation can act as a guide for future legislation.[52] Finally, regulatory agencies could change the way they address data brokers. For example, regulatory agencies could require express permission from consumers for each subsequent sale of their data, not just the initial data collection. Some regulators have already started to advocate for such changes as part of a transition from merely procedural privacy protections to substantive limits on data processing.[53]

The Article proceeds in four Parts. Part I reviews Fourth Amendment law governing data disclosed to third parties and surveys emerging markets in private consumer data. Part II demonstrates that private data, such as location data, is not commercially available to the general public. It also contends that nothing about the act of purchasing data from a third party immunizes the government's collection of data from Fourth Amendment scrutiny. Part III posits that consumers do not meaningfully consent to police searches of their data when they disclose personal data to their cellphone apps. Part IV concludes by drawing lessons about the inadequacy of current consumer privacy law and the interoperability of private and public data surveillance. It then examines several potential solutions to the current lack of legal protections against government purchases of sensitive private data.

I. BACKGROUND AND CONTEXT

A. Third-Party Data

The Supreme Court has held that a Fourth Amendment search occurs when a government official violates a person's "reasonable expectation of privacy"[54] or physically intrudes on certain types of property.[55] Courts have applied different models and theories of what

52. *See infra* notes 367–73 and accompanying text.

53. Lina M. Khan, Chair, Fed. Trade Comm'n, Remarks as Prepared for Delivery at the IAPP Global Privacy Summit 2022 (Apr. 11, 2022) [hereinafter Lina Khan Remarks], http://www.ftc.gov/system/files/ftc_gov/pdf/Remarks%20of%20Chair%20Lina%20M.%20Khan%20at%20IAPP%20Global%20Privacy%20Summit%202022%20-%20Final%20Version.pdf.

54. This standard is often referred to as the *Katz* test, having first appeared in Justice Harlan's concurrence in 1967's *Katz v. United States*, 389 U.S. 347, 360–61 (1967).

55. *See* Florida v. Jardines, 569 U.S. 1, 6–9 (2013); United States v. Jones, 565 U.S. 400, 404–06 (2012). The physical intrusion test has thus far added little to the reasonable expectation of privacy test, and the Supreme Court cases where it has been used may have come out similarly under *Katz*. *See Jardines*, 569 U.S. at 12–16 (Kagan, J., concurring); *Jones*, 565 U.S. at 418–27 (Alito, J., concurring in the judgment).

makes an expectation of privacy reasonable, and the Supreme Court's interpretations of the standard are often inconsistent.[56] But courts generally ask whether an individual's expectation of privacy is one that society would recognize as reasonable.[57] The Supreme Court has also made clear that "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."[58]

Until recently, there were few Fourth Amendment protections for data that a person revealed to other parties. Almost fifty years ago, the Court developed the "third-party doctrine," which provided that a person waives their Fourth Amendment rights in the information they voluntarily disclose to a third party.[59] For example, the Fourth Amendment does not protect bank records associated with a checking account because those records are disclosed to bank employees in the ordinary course of business.[60]

The idea behind the third-party doctrine was that a person who voluntarily disclosed their information to another assumed the risk that the other person might disclose it to the government.[61] This was a plausible assumption in the original third-party doctrine cases, which typically involved suspects voluntarily sharing details of their crimes with undercover government agents.[62] But outside of this face-to-face context, the third-party doctrine has proved controversial.[63] In the internet era, the third-party doctrine

---

56. *See* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503, 541–42 (2007); Matthew Tokson, *The* Carpenter *Test as a Transformation of Fourth Amendment Law*, 2023 U. ILL. L. REV. 507, 513–15 (2023).

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

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

59. The third-party doctrine was not established in its full form until the 1970s, although cases holding that the Fourth Amendment did not apply to statements made to an undercover officer appeared in the 1960s. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (concluding that a list of dialed phone numbers was not protected by the Fourth Amendment); Hoffa v. United States, 385 U.S. 293, 302 (1966) (ruling that testimony regarding statements to a secret government informant was allowable under the Fourth Amendment); Lopez v. United States, 373 U.S. 427, 437–40 (1963) (holding that an electronic recording device that was not unlawfully planted by physical invasion did not violate defendant's Fourth Amendment rights).

60. United States v. Miller, 425 U.S. 435, 444–45 (1976) (holding that a bank customer had no reasonable expectation of privacy in his bank records because they were disclosed to third-party employees).

61. United States v. White, 401 U.S. 745, 749 (1971) (plurality opinion).

62. *Id.* at 746–47; *Lopez*, 373 U.S. at 428–29.

63. *See, e.g.*, Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. U. L. REV. 1441, 1475–80 (2017) (asserting that the third-party doctrine as applied in a digital context undermines the core values of the Fourth Amendment); Jack M. Balkin, *The Constitution in the National Surveillance State*, 93 MINN. L. REV. 1, 19–20 (2008) (characterizing Fourth Amendment

threatens to eliminate privacy protections for a vast swath of personal information, including web-surfing data, communications metadata, medical and biometric data, cloud-stored documents, and location information.[64] These and many other forms of digital information are regularly disclosed to third-party service providers.[65] Under the classic third-party doctrine, government investigators could obtain enormous quantities of personal information without a warrant.[66]

B. Location Data

The Supreme Court eventually reexamined the third-party doctrine in a landmark 2018 case. In *Carpenter v. United States*,[67] the Court held that the government's warrantless acquisition of a suspect's cellphone location data violated the Fourth Amendment.[68] The Court limited the third-party doctrine, deeming it inapplicable to cellphone location data stored by a third party.[69]

It did so on several grounds. The location tracking at issue was pervasive and detailed, potentially revealing a great deal about a person's life and activities.[70] The amount of location data implicated was also massive, as cellphone companies had access to a "detailed chronicle of a person's physical presence compiled every day, every moment, over several years."[71] Cellphone tracking was also "remarkably easy, cheap, and efficient," capable of accessing vast repositories of personal data at little cost to government inspectors.[72] Finally, cellphone location data was not really voluntarily disclosed

---

protections for personal data as weak due to the third-party doctrine); Sherry F. Colb, *What Is a Search? Two Conceptual Flaws in Fourth Amendment Doctrine and Some Hints of a Remedy*, 55 STAN. L. REV. 119, 132–39 (2002) (criticizing the third-party doctrine's risk and exposure-based rationales).

64. *See, e.g.*, Tokson, *supra* note 27, at 585 (noting that third-party doctrine precedents are problematic in an age where individuals store enormous amounts of personal information on various third-party platforms).

65. *See id.*; *see also* Tokson, *supra* note 43, at 1799.

66. Such data is regularly stored in databases and made available to the government upon request or subpoena. *See* Tokson, *supra* note 27, at 585.

67. 138 S. Ct. 2206 (2018).

68. *Id.* at 2221, 2223. Cellphones emit radio waves that communicate with cellphone towers. *Id.* at 2211–12. Cellphone companies can generate a record of a user's location by tracking which cell towers (and which tower antennae) receive a cellphone's signal. They collect this data for various purposes, including selling the data to third parties for marketing purposes. *See id.* For further discussion of cell site location information (CSLI) and cellphone provider data retention practices, see Matthew Tokson, *Knowledge and Fourth Amendment Privacy*, 111 NW. U. L. REV. 139, 160–61 (2016).

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

70. *Id.* at 2217–18.

71. *Id.* at 2220.

72. *Id.* at 2217–18.

to the cellphone companies.[73] Rather, the location data was automatically transmitted to the cell service provider whenever the phone was turned on.[74] And owning a cellphone itself, while technically voluntary, is largely inescapable because owning a cellphone has become practically "indispensable to participation in modern society."[75]

Carpenter is a transformative case, one that may ultimately extend Fourth Amendment protections to a wide variety of sensitive digital information.[76] It has been hailed as a "revolution,"[77] a "landmark privacy case,"[78] a "show-stopper,"[79] and a "major victory for digital privacy."[80] Lower courts have adopted *Carpenter* in hundreds of subsequent cases, charting new courses for Fourth Amendment law and addressing a bevy of novel surveillance technologies.[81] An emerging "*Carpenter* test" employing the factors discussed in the Court's opinion may even someday displace the vague "reasonable expectation of privacy" standard as the primary test for Fourth Amendment searches.[82]

Yet *Carpenter*'s impact is substantial even on its own terms. It prohibits the government from tracking people's locations by obtaining data from their cellphone companies.[83] Long-term location tracking can be deeply revealing of the private details of people's lives.[84] Cellphones are especially prone to revealing such information because they seldom leave their owner's side, tracking their

---

73. *Id.* at 2220.

74. *See id.* at 2211–12, 2220.

75. *Id.* at 2220.

76. *E.g.*, Matthew Tokson, *Telephone Pole Cameras Under Fourth Amendment Law*, 83 OHIO ST. L.J. 977, 982 (2022).

77. *See* Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 378–385 (2019).

78. Rachel Levinson-Waldman, *Supreme Court Strengthens Digital Privacy*, BRENNAN CTR. FOR JUST. (June 22, 2018), http://www.brennancenter.org/our-work/analysis-opinion/supreme-court-strengthens-digital-privacy.

79. Lior Strahilevitz & Matthew Tokson, *Ten Thoughts on Today's Blockbuster Fourth Amendment Decision — Carpenter v. United States*, CONCURRING OPS. (June 22, 2018), http://perma.cc/Y94X-PTXR.

80. Ren LaForme, *The Supreme Court Just Struck a Major Victory for Digital Privacy*, POYNTER (June 25, 2018), http://www.poynter.org/tech-tools/2018/the-supreme-court-just-struck-a-major-victory-for-digital-privacy.

81. Tokson, *supra* note 43, at 1795, 1821.

82. Tokson, *supra* note 56, at 511.

83. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018).

84. *Id.* at 2217. It "provides an intimate window into a person's life, revealing not only his particular movements, but through them his familial, political, professional, religious, and sexual associations." *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring) (internal quotation marks omitted)).

movements almost exactly.[85] This was mitigated somewhat by the relative imprecision of cell site tracking technology, which at the time of *Carpenter* could only place an individual within a one-eighth to four-square-mile area.[86] Nonetheless, and especially in combination with other information, this location data was profoundly revealing of an individual's life.[87] By tracking the cellphones that follow us everywhere in the modern world, the government can achieve "near perfect surveillance."[88]

Carpenter imposed a constitutional check on this powerful form of surveillance, requiring the government to get a warrant before obtaining an individual's cellphone location data from their service provider.[89] But in an era of ubiquitous data collection by private parties, the government may be able to track people's locations by other means. The government can often purchase location data from specialized data vendors.[90] Depending on the legality of these purchases, the government may be able to circumvent *Carpenter*'s restrictions and track individuals' locations without constitutional restraint. As the next Subpart describes, many government entities have already begun to track cellphone users via purchased data.

C. The Government in Data Markets

Several federal agencies and local police departments have purchased private location data from data brokers following *Carpenter v. United States*.[91] For example, ICE purchased $190,000 worth of licenses from the specialized location data broker firm Venntel.[92] This allowed it to access cellphone location data collected from cellphone apps, such as weather, shopping, or game apps.[93] This location data tends to be far more precise than the cell site location information ("CSLI") at issue in *Carpenter*—it can pinpoint an individual's location within a few yards rather than a broad area of hundreds of feet or more.[94] ICE used this data to track the movements of potentially undocumented immigrants near the United States' southern border, and the data

85. *Id.* at 2218. A cellphone "faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales." *Id.*

86. *Id.*

87. *Id.*

88. *Id.*

89. *Id.* at 2223.

90. *See infra* Subpart I.C.

91. 138 S. Ct. 2206 (2018).

92. Tau & Hackman, *supra* note 1.

93. *Id.*

94. *See* Valentino-DeVries et al., *supra* note 27 (reporting that cellphone app location data was "accurate to within a few yards and in some cases updated more than 14,000 times a day"); *Carpenter*, 138 S. Ct. at 2218 (noting that CSLI could locate an individual within a one-eighth to four-square-mile area).

ultimately led to arrests and deportations.[95] It was also used to enforce drug laws, as ICE shared its intelligence with local police departments.[96] Yet ICE and other federal agencies have taken steps to conceal their use of location tracking services from the public, generally keeping mention of the tracking out of police records and court proceedings.[97]

One of the most interesting aspects of ICE's purchase of private location data is its timing. Government records reveal that ICE purchased licenses with Venntel on August 07, 2018—roughly one month after the Supreme Court issued its groundbreaking opinion in *Carpenter*.[98] In light of this timing, and ICE's previously documented use of cell site simulators to track suspects' locations,[99] it seems likely that the agency purchased this data as a means of tracking individuals without complying with *Carpenter*'s requirements.

Other federal agencies also purchase data from specialized brokers.[100] U.S. Customs and Border Protection ("CBP"), which likewise uses location data in immigration enforcement, also purchased Venntel's location tracking services.[101] It has used this data to monitor over 300,000 locations across North America, including parts of many major U.S. cities.[102] The Defense Intelligence Agency ("DIA") also began buying location data after the Supreme Court issued its opinion in *Carpenter*.[103] A request for data from Senator Ron Wyden to the DIA noted that the agency "first started

---

95. Tau & Hackman, *supra* note 1.

96. *See supra* notes 4–7.

97. *See supra* note 7 and accompanying text; *see infra* notes 137–41 and accompanying text.

98. *See Purchase Order (PO) PIID 70CMSD18P00000127, Department of Homeland Security and Venntel Inc*, USASPENDING (Aug. 7, 2018), http://www.usaspending.gov/award/CONT_AWD_70CMSD18P00000127_7012_-NONE-_-NONE-. The *Carpenter* opinion was released on June 22, 2018. Carpenter v. United States, 138 S. Ct. 2206 (2018).

99. Robert Snell, *Feds Use Anti-Terror Tool to Hunt the Undocumented*, DETROIT NEWS (May 19, 2017, 6:18 PM), http://www.detroitnews.com/story/news/local/detroit-city/2017/05/18/cell-snooping-fbi-immigrant/101859616.

100. In addition to those described below, the IRS Criminal Investigations division briefly used Venntel's services from 2017 to early 2018. Tau, *supra* note 15; *see also infra* note 106.

101. Tau & Hackman, *supra* note 1.

102. Alfred Ng, *Homeland Security Records Show 'Shocking' Use of Phone Data, ACLU Says*, POLITICO (July 18, 2022, 3:30 PM), http://www.politico.com/news/2022/07/18/dhs-location-data-aclu-00046208. Its use of this data is apparently ongoing, as the CBP recently renewed a location data service contract. *Id.*

103. Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 25, 2021), http://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html.

buying this source of data" in mid-2018, when *Carpenter* was handed down.[104]

Several federal agencies, including the Secret Service and the State Department, have purchased a service called Locate X, which allows investigators to track mobile devices using information drawn from popular mobile apps.[105] The agencies used this data to investigate, among other things, allegations of credit card fraud at gas station pumps.[106] As with ICE's use of Venntel, the agencies have largely kept the use of this technology a secret and taken steps to avoid public disclosure.[107]

The use of location tracking services in law enforcement is not confined to federal agencies. In recent years, local police departments in cities big and small have purchased location tracking services that enable them to follow people's movements for long periods of time.[108] Many of these police departments have purchased a service named Fog Reveal, which uses cellphone app data culled from over 250 million cellphones.[109] This data is used to create location analyses of

---

104. *Clarification of Information Briefed During DIA's 1 December Briefing on CTD*, DEF. INTEL. AGENCY (Jan. 15, 2021), http://www.wyden.senate.gov/imo/media/doc/011521%20CTD%20Discussion%20RFI%20Response.pdf. The timeline reflected in the request for data is not exact, and it is possible, though unlikely, that the DIA began purchasing cellphone location information just before *Carpenter* was handed down. Even in that unlikely scenario, the purchases were likely made in anticipation of an adverse outcome. *See, e.g.*, Amy Howe, *Argument Analysis: Drawing a Line on Privacy for Cellphone Records, but Where?*, SCOTUSBLOG (Nov. 29, 2017, 2:43 PM), http://www.scotusblog.com/2017/11/argument-analysis-drawing-line-privacy-cellphone-records (noting that the majority of Justices seemed likely to rule in Carpenter's favor); Matthew Feeney, *Thoughts on* Carpenter v. US *Oral Argument*, CATO INST. (Nov. 27, 2017), https://www.cato.org/commentary/thoughts-carpenter-v-us-oral-argument.

105. *See* Charles Levinson, *Through Apps, Not Warrants, 'Locate X' Allows Federal Law Enforcement to Track Phones*, PROTOCOL (Mar. 5, 2020), http://www.protocol.com/government-buying-location-data. Other agencies, including the Department of Justice, the U.S. Marshals Service, the Drug Enforcement Administration, and the Department of Transportation, have contracts with Babel Street, the company that sells Locate X. *Id.* Little is known about these agencies' use of Babel Street's services, and they have declined to comment on this issue when faced with media inquiries. *See id.*

106. *Id.* These investigations ultimately led to arrests of alleged fraudsters. *Id.*

107. *Id. See infra* notes 139–42 and accompanying text.

108. Burke & Dearen, *supra* note 8.

109. *Id.* Fog Reveal works by tracking cellphone users via their advertising IDs, which are unique numbers assigned to each cellphone. These numbers do not identify the user, but cellphones can easily be traced to homes and workplaces in order to identify users. *Id.* Fog Reveal obtains data from popular apps including Waze and Starbucks' app. *Id.*

individuals known as "patterns of life,"[110] and it can stretch back in time several years and forward in time as long as the department keeps paying for the service.[111] Police departments have praised Fog Reveal for allowing them to quickly obtain detailed location information without a warrant, which can be helpful in criminal investigations.[112] The program, which is generally far more affordable than Venntel or Locate X's services, offers "a mass surveillance program on a budget."[113]

Fog Data Science, the company that sells Fog Reveal, often helps law enforcement to deanonymize cellphone users, connecting cellphone records to people's identities.[114] Both Fog Data Science and Venntel have worked closely with police officers during investigations, according to emails obtained in FOIA requests.[115] Like federal agencies, local police departments also generally keep any mention of Fog Reveal or its data out of court records, denying defendants an opportunity to challenge it.[116]

A wide variety of government agencies and police departments are purchasing location tracking services in order to closely monitor the movements of cellphone users for a variety of purposes.[117] Some targets of this surveillance have committed crimes, and others are innocent parties who happen to be in a location of interest.[118] The volume of this tracking is difficult to quantify, because government officials, with the encouragement of the data vendors, tend to avoid mentioning this surveillance in official records or court proceedings.[119] It occurs instead in the shadows of investigation, generating leads that police officers can use to pull over suspects pretextually,[120] or monitoring innocent people and failing to generate leads at all.[121] But the sheer number of agencies and police departments that purchase location tracking services, and the large amounts of money spent, suggest increasingly widespread use.[122]

---

110. *Id.* This phrase, used by law enforcement to describe location tracking, parallels the Supreme Court's description of cellphone tracking as revealing the "privacies of life." Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

111. Burke & Dearen, *supra* note 8.

112. *Id.*

113. *Id.* (quoting a special adviser for the Electronic Frontier Foundation).

114. Burke & Dearen, *supra* note 8.

115. *Id.*

116. *Id.* Fog Data Science has encouraged this approach in public statements. *Id*.

117. *See id*.

118. *See id.*

119. *See id.*; Tau & Hackman, *supra* note 1; Levinson, *supra* note 105.

120. Tau & Hackman, *supra* note 1.

121. *See* Burke & Dearen, *supra* note 8.

122. *See, e.g.*, Levinson, *supra* note 105 (detailing the millions of dollars spent on location tracking services by the federal government and describing an increase in spending over time); Burke & Dearen, *supra* note 8 (describing a

Going forward, the legality of this form of location tracking is likely to dictate whether Americans can maintain privacy in their movements and activities against government observation. And while location surveillance is the most common focus of law enforcement data purchases today, the principles that govern location data will also apply to the myriad other forms of sensitive data that cellphones collect.[123]

Indeed, government agencies have already begun to purchase sensitive non-location data.[124] For example, military intelligence agencies recently purchased large quantities of internet traffic log data from a private broker, allowing them to track the activity of hundreds of millions of United States internet users.[125] Using a service called Augury sold by the Argonne Ridge Group, these agencies are able to access billions of IP address netflow records.[126] These records detail the servers and computers with whom an individual internet user connects, often disclosing particular websites and email addresses contacted.[127] Such data can be extremely revealing of a user's interests and their personal, financial, sexual, and political activities.[128] This is only one example of government agencies purchasing internet surfing data from brokers; other examples are gradually emerging from sources like DOJ investigation files and emails obtained via open records laws.[129] The scale and

---

variety of states, cities, counties, and small towns purchasing location tracking services); Joseph Cox, *Here Is the Manual for the Mass Surveillance Tool Cops Use to Track Phones*, VICE (Sept. 1, 2022, 1:39 PM), http://www.vice.com/en/article/v7v34a/fog-reveal-local-cops-phone-location-data-manual (listing additional police departments that use location tracking services); Cyphers, *supra* note 8 (listing additional police agencies that use location tracking services and evidence that Fog Data Science works with many more).

123. *See infra* notes 30 and accompanying text (discussing numerous forms of intimate data collected by cellphone and internet service providers).

124. Cameron & DeGeurin, *supra* note 17.

125. *Id.*

126. *Id.*

127. *Id.* The service even allows the government to follow traffic through virtual private networks ("VPNs"), which are used by some individuals to enhance privacy while surfing the internet. *Id.*

128. *See id.*; Tokson, *supra* note 27, at 628.

129. *See, e.g.*, Menn, *supra* note 17 (describing purchases of web-surfing data by law enforcement and intelligence agencies); Letter from Ron Wyden, U.S. Sen., to Lina Khan, Chair, Fed. Trade Comm'n (Dec. 15, 2022), http://docs-cdn-prod.news-engineering.aws.wapo.pub/publish_document/027775b4-5d64-4b16-86b1-9f3dbb9d98da/published/027775b4-5d64-4b16-86b1-9f3dbb9d98da.pdf (describing how purchases of web-surfing data by government agencies came to public attention); Letter from Ron Wyden, U.S. Sen., & Cynthia M. Lummis, U.S. Sen., to Merrick Garland, Att'y Gen. (Mar. 29, 2023), http://s3.documentcloud.org/documents/23729538/wyden-letter-sources.pdf (discussing the government's unregulated purchases of passenger manifest data

breadth of government purchases of private data appears to be vast—and growing.

II. GOVERNMENT PURCHASES AND FOURTH AMENDMENT LAW

The Supreme Court has held that "an individual maintains a legitimate expectation of privacy in the record of his physical movements" as captured by cellphone location data.[130] Set aside, for now, any differences between the CSLI at issue in *Carpenter* and the cellphone app data purchased by the government.[131] Does otherwise private data lose its Fourth Amendment protection because the government purchases it from a private company?

It is a complex and novel issue, but ultimately Fourth Amendment law and the principles that undergird it require the government to obtain a warrant before purchasing private data. There is, in other words, nothing special about purchases that permits the government to obtain otherwise protected data without a warrant. When the government purchases sensitive data, otherwise shielded from public observation, that data remains protected by the Fourth Amendment.

In the context of cellphones, the Fourth Amendment continues to protect location data from warrantless government observation, even though the government can purchase such data from specialized vendors. This data is not publicly exposed or accessible. It is available only to government agencies, or in large, anonymized blocks of data processed by corporate entities and inaccessible to the public.[132] It would be virtually impossible for most members of the public to obtain or use such data. Further, even if the data were to become accessible to the general public, it would likely remain functionally private, with few people actually using the technology. So long as personalized data remains functionally private, it retains its constitutional protections under current law.[133]

A. Limited Commercial Availability

Government agencies have justified their purchases of personal location data on the grounds that such data is commercially available, and accordingly the government can purchase it without constitutional restriction.[134] But, while the government does purchase this data from private entities, the data is not publicly available or exposed.

---

from private bus and airline companies and payments to shipping industry employees in exchange for opening sealed packages in transit).

130. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018).

131. These differences will be addressed *infra* Part III.

132. Tau & Hackman, *supra* note 1.

133. *See infra* Subpart II.B.

134. *See supra* note 15.

Members of the public cannot purchase location tracking data from the vendors that sell location data to the government. These vendors typically sell location data exclusively to law enforcement agencies.[135] Companies like Venntel, the vendor that sold data to the IRS and the Department of Homeland Security, are not consumer-facing.[136] They market their tracking services to the "public sector," i.e., to government entities.[137] Such companies go to great lengths to avoid publicly disclosing information about their services or their clients.[138] Babel Street, which sells the location tracker Locate X to several federal agencies, goes even further, keeping its location tracking services confidential via a series of non-disclosure clauses and other contractual restrictions.[139] For example, it contractually forbids federal agencies from introducing its location data as evidence or mentioning it at all in legal proceedings.[140] The agencies can use the data to generate leads or informally tip off local investigators, but they cannot use it in court—denying courts any opportunity to rule it unlawful.[141] This policy likewise denies defendants any opportunity to challenge the use of Locate X against them.[142]

Babel Street also emphasizes that it does not sell its tracking service to commercial clients and limits its sales to federal agencies involved in law enforcement and national security.[143] Even Fog Reveal, which tends to be used by local police departments, is not public facing. Access to any part of its website is restricted to "[o]nly authorized users" who agree to be "governed by their agency/sponsor's

---

135. Tau & Hackman, *supra* note 1.

136. *Id.*

137. Levinson, *supra* note 105.

138. *See supra* notes 7 and accompanying text.

139. Levinson, *supra* note 105.

140. *Id.*

141. *See id.* (quoting a former government official familiar with Locate X on how it can be used to generate leads that investigators can then verify through other means).

142. *Id.* (quoting ACLU attorney Nathan Wessler's observation that "These secrecy provisions prevent the courts from providing oversight . . . [t]hat is really corrosive to our system of checks and balances."); *see also* State v. Andrews, 134 A.3d 324, 339 (Md. Ct. Spec. App. 2016) (stating in a case involving a nondisclosure agreement around an earlier form of location tracking technology that "[w]e perceive the State's actions in this case to protect the [] technology, driven by a nondisclosure agreement to which it bound itself, as detrimental to its position and inimical to the constitutional principles we revere"). Some federal agencies have declined to use the service after their lawyers expressed concerns about its legality. Levinson, *supra* note 105.

143. Levinson, *supra* note 105.

policies and guidelines."[144] Fog Reveal also forbids search engines from printing a description of its website.[145]

These companies are not stores open to the public; they are specialized contractors providing sensitive data to law enforcement. These contractors likely have little motivation to open their businesses to a broad customer base. Providing detailed information about individuals' movements might expose these companies to punitive regulatory enforcement actions if such information were used by stalkers or abusive partners.[146] Indeed, such data may have relatively few lawful applications. Access to personalized location tracking services would also be far too expensive for most people. A Venntel license would cost hundreds of thousands of dollars per year.[147] Fog Reveal is more affordable, but even basic access to that service costs at least $7,500 annually.[148] Even if individual licenses were cheaper than institutional licenses, they would likely be prohibitively expensive for most consumers.

Location data is also sold commercially to help facilitate targeted advertising, with data vendors selling large, anonymized blocks of data, typically to marketers and ad companies.[149] This data is often precise, and it could permit an expert to deanonymize a particular target, for example by tracing them to their home and using their

144. FOG REVEAL, http://www.fogreveal.com/App/Login (last visited Feb. 13, 2024).

145. For example, Google results report that "[n]o information is available for this page" because "the website prevented Google from creating a page description." GOOGLE, https://www.google.com/search?q=fogreveal.com&rlz=1C1VDKB_enUS999US999&oq=fog+reveal&aqs=chrome..69i57j0i512l9.1322j0j7&sourceid=chrome&ie=UTF-8; *No Page Information in Search Results*, GOOGLE HELP, http://support.google.com/webmasters/answer/7489871?hl=en (last visited Feb. 13, 2024). A Bing search yields similar results, noting under the website's URL that "[w]e would like to show you a description here but the site won't allow us." MICROSOFT BING, https://www.bing.com/search?q=fogreveal.com&qs=n&form=QBRE&sp=-1&ghc=1&lq=0&pq=fogreveal.com&sc=3-13&sk=&cvid=7152815A7DF049D28458FDD7D90FABE8&ghsh=0&ghacc=0&ghpl= (last visited Feb. 13, 2024).

146. *See* DANIELLE KEATS CITRON, THE FIGHT FOR PRIVACY 100–01 (2022) (discussing regulatory enforcement actions against stalkerware companies). Recently, the FTC entirely banned a spy software company from operating. *See FTC Bans SpyFone and CEO from Surveillance Business and Orders Company to Delete All Secretly Stolen Data*, FED. TRADE COMM'N (Sept. 1, 2021), http://www.ftc.gov/news-events/news/press-releases/2021/09/ftc-bans-spyfone-ceo-surveillance-business-orders-company-delete-all-secretly-stolen-data.

147. Tau & Hackman, *supra* note 1.

148. Burke & Dearen, *supra* note 8.

149. *See supra* note 27.

address and other information to identify them.[150] But it is not designed or processed for individualized tracking, and in any event is not available to the general public.[151] Take notorious data vendor SafeGraph, the subject of a news story about its controversial sales of location information involving cellphone users visiting abortion clinics.[152] SafeGraph's collection of this sensitive information was concerning in the post-*Dobbs* legal environment, where women might potentially face prosecution or discrimination for visiting an abortion clinic.[153] But SafeGraph's data would have been difficult for even the most skilled user to deanonymize. Its data did not report on individual device movement but rather gave aggregated numbers on the movement of groups of devices; did not report individual residential addresses but only aggregate movements to census blocks; and was limited to the locations users came from immediately before arriving at a target location and where users travelled to immediately

150. *See* Valentino-DeVries et al., *supra* note 27. In addition, some data brokers offer access to data that can link cellphone advertiser ID numbers to personally identifiable information such as names and street addresses. Joseph Cox, *Inside the Industry That Unmasks People at Scale*, VICE (July 14, 2021, 9:00 AM), http://www.vice.com/en/article/epnmvz/industry-unmasks-at-scale-maid-to-pii. It is unclear how accurate or thorough this data is, or whether its sale is legal. *See id.*

151. In one exceptional instance, a non-profit organization called Catholic Laity and Clergy for Renewal spent millions of dollars and a substantial amount of time and manpower to purchase and analyze data from Grindr and other gay dating apps, in order to expose gay Catholic priests using the apps. Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data that Tracked Gay Priests*, WASH. POST (Mar. 9, 2023, 8:52 AM), http://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops. However, Grindr, Growler, and other dating apps involved in the story have stopped disclosing location information to third-party advertisers. *Id.* A data broker whose lax verification system in theory allowed individuals to pose as businesses and thereby purchase its detailed location data which they might in theory deanonymize was sued by the FTC for engaging in unfair business practices. *See* Complaint for Permanent Injunction and Other Relief at 1, 2, FTC v. Kochava Inc., No. 2:22-cv-377 (D. Idaho, Aug. 29, 2022). The FTC's allegations against the data broker were phrased as hypothetical, and the agency did not identify any instances of an individual actually acquiring or using sensitive location data. *Id.*

152. Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE (May 3, 2022, 12:46 PM), http://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood.

153. Geoffrey A. Fowler & Tatum Hunter, *For People Seeking Abortions, Digital Privacy is Suddenly Critical*, WASH. POST (June 24, 2022, 4:23 PM), http://www.washingtonpost.com/technology/2022/05/04/abortion-digital-privacy.

after.[154] Many companies take similar steps to obscure user identities.[155]

SafeGraph's data is available only to corporate clients, not the general public—purchasing it requires leaving a work email and company name with the website, and then scheduling a demonstration with a sales representative who will show you "what [their] data can do for your business."[156] And if a corporate client wants to track consumers to and from a target location, even they are now out of luck.[157] SafeGraph's foot traffic data is no longer available as of the start of 2023, as the company has decided to limit itself to less controversial forms of data.[158]

A similar analysis would likely apply to most non-location data purchased for surveillance purposes. Data revealing the IP addresses of the websites an individual IP address visits is not commercially available to the public, but appears to be specifically marketed to government entities.[159] Access to similar, anonymous data might be sold to corporate entities for cybersecurity purposes or to commercial entities for fraud prevention purposes.[160] The brokers selling such data are not public facing and typically require a company name, company email, and lawful purpose to begin the corporate sales process.[161]

In short, cellphone and other digital data designed for personalized surveillance is sold to government agencies, not the

---

154. Cox, *supra* note 152. The lack of continuous data points could thwart even advanced and labor-intensive deanonymization methods, which may require more data points. *See* Yves-Alexandre de Montjoye et al., *Unique in the Crowd: The Privacy Bounds of Human Mobility*, 3 SCI. REPS. 1, 2–3 (2013) (reporting on advanced deanonymization techniques that used relatively few, albeit precise, location coordinates coupled with data from social media, public records, and other sources).

155. Valentino-DeVries et al., *supra* note 27.

156. *See* SAFEGRAPH, https://www.safegraph.com/schedule-a-demo (last visited Feb. 13, 2024).

157. *See Patterns*, SAFEGRAPH, http://docs.safegraph.com/docs/monthly-patterns (last visited Feb. 13, 2024) (referring to such data as a "Legacy Product" and stating that clients seeking consumer tracking should contact the company for a referral "to a mobility data partner").

158. *See id.* (noting that its website "references SafeGraph Patterns, Weekly Patterns, and/or Neighborhood Patterns, legacy products that will no longer be available at the start of 2023").

159. *See* Cameron & DeGeurin, *supra* note 17.

160. *See, e.g.*, Alfred Ng, *Data Brokers Raise Privacy Concerns — But Get Millions from the Federal Government*, POLITICO (Dec. 21, 2022, 4:30 AM), http://www.politico.com/news/2022/12/21/data-brokers-privacy-federal-government-00072600; Suresh Dakshina, *Analyzing IP Addresses to Prevent Fraud*, CHARGEBACK GURUS (Apr. 26, 2022), http://www.chargebackgurus.com/blog/analyzing-ip-addresses.

161. *See, e.g.*, TEAM CYMRU, http://www.team-cymru.com/contact-sales (last visited Feb. 13, 2024).

general public. The specialized services that work with the government to track individuals do not sell their services to the public and actively avoid public disclosure of their activities.[162] Data in aggregated blocks, suitable for market research, fraud prevention, or advertising purposes, is not sold to the public and is often unsuitable for personalized tracking.[163] Thus, the data used by the government for surveilling suspects is not commercially available to the general public.

B. The General Public Use Standard

What if detailed cellphone location or other personal information were to become available for sale to the general public? Or what if a court were to deem it publicly available on the basis of its sale in anonymized blocks to commercial entities? Unless such information were routinely purchased by actual members of the public, it would remain protected by the Fourth Amendment. Of course, the Supreme Court has not yet weighed in on the constitutionality of government purchases of sensitive private data. But it has previously ruled on an invasive technology that was available to the public but not widely used.

In *Kyllo v. United States*,[164] the Supreme Court confronted a new surveillance technology: infrared heat cameras, which could capture the heat signatures emitted from a house and thereby reveal some of the activities inside.[165] For example, in the case itself, the police were able to determine that a homeowner was using marijuana grow lamps inside his house by using the infrared cameras.[166] These cameras were "readily available to the public" for purchase or rental.[167] In addition, longstanding property doctrines dictated that visual surveillance from public areas was not a trespass, and longstanding Fourth Amendment doctrines had held that it was not a search.[168] Yet the Court recognized that advancing surveillance technology required Fourth Amendment scrutiny if individual privacy was to be preserved.[169] The Court held that the warrantless use of infrared

162. *See supra* notes 135–43 and accompanying text.

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

164. 533 U.S. 27 (2001).

165. *Id.* at 29.

166. *Id.* at 29–30.

167. *Id.* at 47 n.5 (Stevens, J., dissenting). Today, these cameras are broadly available, although still not widely used by the public, and are typically employed by contractors to detect anomalous heat signatures, active electrical wires, or HVAC problems. *See, e.g.*, Scott Dutfield, *Infrared Cameras: Invention and Uses*, LIVE SCIENCE (Apr. 5, 2022), http://www.livescience.com/infrared-camera.

168. *Kyllo*, 533 U.S. at 31–32; Boyd v. United States, 116 U.S. 616, 628 (1886) (quoting Entick v. Carrington, 19 Howell's State Trials 1029, 95 Eng. Rep. 807 (K.B. 1765)).

169. *Kyllo*, 533 U.S. at 34–35.

cameras violated the Fourth Amendment, at least so long as they were not in "general public use."[170]

The general public use exception has been criticized as under-protective of privacy; many scholars have argued that the police should not take revealing thermal images of a house regardless of whether members of the public generally do so.[171] There may be room in the concept of a "reasonable expectation of privacy," or under the *Carpenter* factors, for a rule that the police cannot perform some surveillance practices without a warrant even if private parties regularly engage in the same practices. But the Court has never reached this conclusion, and it need not make any such ruling in the context of purchases of sensitive private data. In addition, the Court's precedents arguably required the "general public use" caveat, because the Court had previously held that overflight observation of a backyard was not constitutionally forbidden, since flights in the public airways were routine.[172] Because the Court could "quite confidently say that thermal imaging is not routine," it found that the heat signature of a home remained constitutionally protected.[173]

A similar analysis would apply if, for example, detailed cellphone location data were to be deemed publicly available. Detailed location data is sensitive and revealing, worthy of constitutional protection, and previously protected under *Carpenter v. United States*.[174] This data, while commercially available in theory, is functionally private, because no members of the public and only a few specialized marketing entities access it.[175] When the government purchases an individual's detailed location data from a surveillance vendor, it violates that individual's privacy. Unless the government obtains a warrant before doing so, it conducts an unlawful search under the Fourth Amendment.[176]

---

170. *Id.* at 34.

171. *See, e.g.*, Richard Sobel, Barry Horwitz & Gerald Jenkins, *The Fourth Amendment Beyond* Katz*,* Kyllo *and* Jones*: Reinstating Justifiable Reliance as a More Secure Constitutional Standard for Privacy*, 22 B.U. PUB. INT. L.J. 1, 16 n.93 (2013); Raymond Shih Ray Ku, *The Founders' Privacy: The Fourth Amendment and the Power of Technological Surveillance*, 86 MINN. L. REV. 1325, 1378 (2002); Tracey Maclin, Katz, Kyllo, *and Technology: Virtual Fourth Amendment Protection in the Twenty-First Century*, 72 MISS. L.J. 51, 105 (2002).

172. *Kyllo*, 533 U.S. at 39 n.6 (quoting California v. Ciraolo, 476 U.S. 207, 215 (1986)).

173. *Id.* (internal quotation marks omitted).

174. *See* Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); *see also* discussion *infra* Subpart III.D.

175. *See supra* Subpart II.A.

176. *See* Katz v. United States, 389 U.S. 347, 353, 358–59 (1967) (finding that the police violated Katz's privacy without first securing the necessary search warrant).

To be sure, *Kyllo* involved the observation of a house, and houses are considered especially private in Fourth Amendment law.[177] But nothing in *Kyllo* would limit the rationales discussed above to residential property.[178] The *Kyllo* opinion overtly embraced the logic of *Katz v. United States*, which involved a public phone booth, not a home.[179] And the Supreme Court reached a similar holding in *Bond v. United States*,[180] where a government agent's squeezing of a bag in a bus's luggage rack was found to violate the Fourth Amendment, notwithstanding the possibility that such a bag might be touched or handled by a member of the public.[181] The mere possibility of observation by a member of the public, without more, was insufficient to eliminate Fourth Amendment protection.[182] Rather, the government would have to show that such public observation occurred "as a matter of course" in order to prove that passengers had surrendered their privacy.[183] Nor are these the only Supreme Court cases holding that the police cannot engage in surveillance activities that members of the public might in theory undertake, but generally do not.[184]

---

177. *See e.g.*, *Kyllo*, 533 U.S. at 37–40 (discussing the particular protection afforded to the home in Fourth Amendment law); Michigan v. Clifford, 464 U.S. 287, 295 (1984) (holding that homeowners "retained reasonable privacy interests in their fire-damaged residence and that the post-fire investigations were subject to the warrant requirement"); Payton v. New York, 445 U.S. 573, 576 (1980) (holding that the police must obtain a warrant before arresting a suspect in their home). *But see* Ric Simmons, Lange*,* Caniglia*, and the Myth of Home Exceptionalism*, 54 ARIZ. ST. L.J. 145, 148 (2022) ("Fourth Amendment jurisprudence does not provide the home with significantly greater protection than other types of private property.").

178. *See Kyllo*, 533 U.S. at 34–40.

179. The *Kyllo* Court relied on the idea that "[w]e rejected . . . a mechanical interpretation of the Fourth Amendment in *Katz* . . . [r]eversing that approach would leave the homeowner at the mercy of advancing technology . . . ." *Id.* at 35; *see also id.* at 34 ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

180. 529 U.S. 334 (2000).

181. *Id.* at 338–39.

182. *Id.* at 338.

183. *Id.* at 339.

184. In *Florida v. Jardines*, the Court held that the physical presence of police officers with drug-sniffing dogs in a defendant's curtilage constituted a Fourth Amendment search. 569 U.S. 1, 11–12 (2013). As the dissent noted, and the majority opinion did not contest, there was nothing about the use of drug-sniffing dogs that would turn an otherwise lawful entry onto curtilage into a trespass. *Id.* at 16–17, 23 (Alito, J., dissenting). Yet the majority held that police entering a person's curtilage with a drug-sniffing dog (or a metal detector) violated the Fourth Amendment because it did not comport with "the background social norms" governing how visitors typically approach front doors. *Id.* at 9. Accordingly, even if approaching someone's door with a drug-sniffing dog or metal detector is perfectly lawful, and even though any member of the public might in

In other words, we need not monitor every data vendor or every data sale, ready to eliminate constitutional protection for private app data the instant some determined individual manages to purchase it.[185] Under the principles of several prior Supreme Court cases, rare instances of public access to sensitive data do not strip the data of its Fourth Amendment protections.[186]

C. Government Purchases and Anti-Evasion Principles

Personal cellphone location data is not publicly available for purchase, and it is certainly not in general public use. But the government does purchase it from specialized third-party vendors. Does the fact that money is exchanged for data remove all Fourth Amendment protections for that data?

It does not. To start with an extreme example, the government could not pay a private company to break into people's homes and catalog everything inside without violating the Fourth Amendment.[187] But a more plausible hypothetical better demonstrates the point. Imagine that Venntel decides to branch out beyond selling cellphone location data and begins selling infrared heat scans of people's houses. Various government agencies pay Venntel for this information. An agent can simply enter a suspect's name and address into Venntel's program, and shortly thereafter they receive detailed images of the heat signature of the suspect's house in exchange for a fee.

This purchase would constitute a Fourth Amendment search. First, courts might consider Venntel to be a state actor, as it is not consumer facing, works collaboratively with the government to identify suspects, and primarily or exclusively serves government clients.[188] State actors cannot lawfully use an infrared camera to surveil a home without a warrant.[189] Second, even if Venntel were not a state actor, the government would be a state actor purposefully obtaining private, protected information about the interior of a home.

---

theory choose to do it, it is not generally done. *Id.* It is, therefore, a violation of the Fourth Amendment for the police to do it without a warrant. *Id.* at 11.

185. Perhaps today, at least in theory, an individual with a great deal of money and time might be able to track an individual by purchasing their location data from a third-party vendor. *Cf. supra* note 151 (describing individualized tracking of priests conducted by a well-financed Catholic non-profit organization). This would not affect the Fourth Amendment analysis, nor should it.

186. *See supra* notes 165–74, 181–85 and accompanying text.

187. Among other issues, the government would be violating the homeowner's reasonable expectation of privacy by obtaining private information about the interior of their house. *See, e.g.*, Payton v. New York, 445 U.S. 573, 586 (1980); Kyllo v. United States, 533 U.S. 27, 34 (2001); Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

188. Levinson, *supra* note 105; Tau & Hackman, *supra* note 1.

189. *See, e.g.*, *Kyllo*, 533 U.S. at 34.

In doing so, they would violate the homeowner's reasonable expectation of privacy in their home and would thereby be conducting a Fourth Amendment search.[190] Nothing about purchasing this sensitive data from a vendor changes that analysis.

Finally, courts frequently apply "anti-evasion" principles to prevent parties from circumventing constitutional rules by employing workarounds or adopting hyper-technical interpretations of constitutional provisions.[191] Courts rely on anti-evasion principles when the government uses regulations rather than direct condemnation to perform a taking, or discriminates against out-of-state commerce via a facially neutral statute, or employs putatively private actors to perform a public function.[192] The idea is that the government cannot make an end-run around every constitutional ruling it dislikes or the Constitution would eventually cease to matter.[193] Under these principles, the government cannot circumvent constitutional protections against the thermal imaging of a home by paying a private party for its functional equivalent.[194] To rule otherwise would permit the government to nullify the Fourth Amendment's protection of the home.[195] Longstanding constitutional principles compel courts to block both overt violations of the Constitution and their functional equivalents,[196] and to remain vigilant against "circuitous and indirect methods" of undermining fundamental rights.[197]

The same principles apply to purchases of cellphone location data. Such data is otherwise protected by the Fourth Amendment, and the government cannot circumvent this protection by purchasing the data from a service provider.[198] Personalized location data is not publicly available nor in general public use, and cellphone users have a reasonable expectation of privacy in it.[199] Purchasing that data violates users' privacy and is accordingly a Fourth Amendment

190. *See id.*; *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

191. *See supra* note 33.

192. Lingle v. Chevron U.S.A. Inc., 544 U.S. 528, 539 (2005); Brentwood Acad. v. Tenn. Secondary Sch. Athletic Ass'n, 531 U.S. 288, 298 (2001); Best & Co. v. Maxwell, 311 U.S. 454, 455–56 (1940); Denning & Kent, *supra* note 33, at 1776–77.

193. *E.g.*, Cummings v. Missouri, 71 U.S. 277, 325 (1866); Denning & Kent, *supra* note 33, at 1776–77.

194. *See Kyllo*, 533 U.S. at 34 (holding that a warrantless infrared imaging of a house violated the Fourth Amendment); *Lingle*, 544 U.S. at 539 (discussing the Constitution's prohibition on the functional equivalents of takings).

195. *See Kyllo*, 533 U.S. at 37–40.

196. *See supra* note 33.

197. Byars v. United States, 273 U.S. 28, 32 (1927); *see supra* note 33.

198. *See infra* Part III; *supra* notes 192–98 and accompanying text.

199. *See supra* Subpart II.A–II.B; Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018); *infra* Part III.

search.[200] Moreover, in line with longstanding constitutional principles, the government cannot sneak its way around *Carpenter v. United States* by purchasing sensitive data that it could not constitutionally collect itself.[201] Indeed, applying anti-circumvention principles is especially important here given that many government agencies began purchasing location data in large quantities almost immediately following the *Carpenter* decision.[202]

1. Co-Tenants and Retail Stores

Arguments that government purchases are immune from Fourth Amendment scrutiny are likely to cite *Maryland v. Macon,*[203] a 1985 case involving pornographic magazines.[204] The Supreme Court held in *Macon* that police officers entering a physical store open to the public was not a search of the store and purchasing an item in the store was not a seizure.[205] But the Court has never addressed whether purchasing private, otherwise constitutionally-protected data is a search. *Macon* did not even address whether the government's purchase of obscene magazines was a search, probably because the magazines were considered contraband and thus there was no possible claim to a reasonable expectation of privacy in them.[206]

---

200. *See supra* note 191 and accompanying text. It might be argued that purchasing and observing the data violates users' privacy, but merely purchasing it alone does not. *See* Tokson, *supra* note 27, at 615–16. However, addressing the purchase of sensitive data as a Fourth Amendment search avoids unnecessary logistical and factual problems across cases and is consistent with decisions like *Carpenter*, which hold that obtaining sensitive data is a search, regardless of later observation. *See Carpenter*, 138 S. Ct. at 2223 ("The Government's acquisition of the cell-site records here was a search . . . ."). The Court's approach may be motivated in part by practical and legal necessity. Once the government obtains protected information, it would be difficult and perhaps impossible for courts to effectively monitor whether government officials subsequently observe the data. *See* Ric Simmons, *The Mirage of Use Restrictions*, 96 N.C. L. REV. 133, 189 (2017).

201. *See Carpenter*, 138 S. Ct. at 2223; *see supra* notes 192–98 and accompanying text.

202. *See supra* notes 101–02, 106–07 and accompanying text; *see also* Burke & Dearen, *supra* note 8 (describing police departments purchasing or inquiring about location tracking services in 2018).

203. 472 U.S. 463 (1985).

204. *Id.* at 465; *see* Kerr, *supra* note 15, at 2–3; Aaron X. Sobel, Note, *End-Running Warrants: Purchasing Data under the Fourth Amendment and the State Action Problem*, YALE L. & POL'Y REV. (forthcoming 2024).

205. *Macon*, 472 U.S. at 469–70.

206. The Court concluded that "the purchase [of the magazine] is analogous to purchases of other unlawful substances previously found not to violate the Fourth Amendment." *Id.* at 470 (citing Lewis v. United States, 385 U.S. 206, 210 (1966)). An individual's cellphone location data is obviously not an "unlawful

It might be argued, based on an analogy to the law governing roommate consent searches, that app companies can waive their users' Fourth Amendment rights by selling their data.[207] If the police approach a house when only one roommate is present and obtain consent to search from that roommate, the search is valid, even if the absent roommate would object.[208] One could argue that an individual's cellphone data is like a house shared between two roommates: the individual and the company who collects their data.[209] Under this analogy, the government can pay (or otherwise convince) a company to provide it with a user's sensitive data, even without the user's permission.[210] So long as the company agrees, the government can obtain *Carpenter*-protected records without having to comply with *Carpenter*'s warrant requirement.[211]

Yet the "roommate" analogy is a poor fit for Fourth Amendment rights in sensitive data. The cohabitation cases are premised on the idea that roommates make common use of the shared property that they mutually inhabit.[212] But cellphone users and the companies that own their data are hardly on the same footing with respect to sensitive data, such as location data. Rather, cellphone users have a privacy right in this data, which concerns them alone, reveals their "familial, political, professional, religious, and sexual associations,"[213] and holds for them the "privacies of life."[214] App companies have no meaningful privacy interest in the data itself, which does not concern them or their employees. And it is the user's privacy interest that *Carpenter* protects, not any tangential property interests they might

---

substance," and the Court has held that it is worthy of Fourth Amendment protection, at least in some contexts. *Carpenter*, 138 S. Ct. at 2223.

207. Kerr, *supra* note 15, at 4–5.

208. *E.g.*, United States v. Matlock, 415 U.S. 164, 171 n.7 (1974). In a house, the police cannot enter and search if one of the two roommates is present and objects to the search. Georgia v. Randolph, 547 U.S. 103, 120 (2006).

209. Kerr, *supra* note 15, at 4 (arguing that companies have common authority over constitutionally protected user data and can consent to a search of that data without permission from the user).

210. When personal data is held by telecom companies such as cellphone providers, these providers may be especially likely to comply with informal government requests for user information, because these companies are extensively regulated and depend in part on government good will. *See, e.g.*, Dennis L. Weisman & Robert B. Kulick, *Price Discrimination, Two-Sided Markets, and Net Neutrality Regulation*, 13 TUL. J. TECH. & INTELL. PROP. 81, 96 (2010) (describing how regulators have permitted certain beneficial rate arrangements to telecom companies).

211. Kerr, *supra* note 15, at 4.

212. *Matlock*, 415 U.S. at 171 n.7 (stating that the concept of common authority rests on the "mutual use of the property by persons generally having joint access or control for most purposes").

213. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012)).

214. *Id.*

have in a third-party company's business records.[215] Only the user has a privacy right in their personal data, and only they can surrender this right.

Neither do cellphone users and the companies that collect their data have a co-equal property right in the companies' business records. Rather, they have divergent property interests and engage in completely different "uses" of the customer's personal data.[216] Companies own the records but virtually never observe individual users' information absent a specific request from law enforcement.[217] Users have no ownership interest, are typically the only human beings who see their own data, and often enjoy certain limited, derivative rights in their records granted by contract or positive law.[218] Accordingly, the closest analogy to pre-internet law is likely the landlord/tenant relationship, where tenants maintain a Fourth Amendment interest in their apartments that their landlords, who actually own the apartments, cannot waive.[219] To allow landlords to give up their tenants' rights "would reduce the Fourth Amendment to a nullity and leave tenants' homes secure only in the discretion of landlords."[220] In the digital era, the same can be said of allowing service providers to waive their customers' rights over personal data.

2. A Case Study

Courts are just beginning to address the complex question of government purchases of sensitive data.[221] But the first such decision in the federal courts found a Fourth Amendment violation when law

---

215. *Id.* at 2214 n.1.

216. *Cf. Matlock*, 415 U.S. at 171 n.7 ("The authority which justifies the third-party consent . . . rests rather on mutual use of the property by persons generally having joint access or control for most purposes.").

217. *See supra* text accompanying notes 23–28; *see also, e.g.*, *Carpenter*, 138 S. Ct. at 2212 (noting that wireless carriers often sell aggregated blocks of location records "without individual identifying information").

218. *See Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting) (describing how federal statutes give cellphone users certain limited rights to control the disclosure of personal information about their cellphone use); Mailyn Fidler, *Warranted Exclusion: A Case for a Fourth Amendment Built on the Right to Exclude*, 76 SMU L. REV. 315, 361–362 (2023) (construing federal statutes partially protecting cellphone users as creating a limited right to exclude).

219. Chapman v. United States, 365 U.S. 610, 616–17 (1961) (holding that a landlord cannot give permission for a Fourth Amendment search of a tenant's home); *see also* Stoner v. California, 376 U.S. 483, 489 (1964) (holding that the police must obtain a search warrant to enter a hotel room despite the fact that "maids, janitors, or repairmen" routinely enter and observe the room in the normal course of business).

220. *Chapman*, 365 U.S. at 617 (quoting Johnson v. United States, 333 U.S. 10, 14 (1948)) (cleaned up).

221. *See infra* Part III.

enforcement officers purchased cellphone location data from a private company.

In *Cooper v. Hutcheson*,[222] a County Sheriff's Department in Missouri purchased a cellphone tracking data service from Securus, a telecommunications company.[223] Plaintiffs sued the sheriffs and Securus under 42 U.S.C. § 1983 for violating their Fourth Amendment rights by tracking their location.[224] The court held that Securus was a state actor for Fourth Amendment purposes.[225] Securus's customers were exclusively law enforcement personnel, and it sold a product designed to help track individuals in criminal investigations.[226] As a result, the court considered Securus "a willful participant in joint activity with the State or its agents," subject to the same Fourth Amendment restrictions as the sheriffs.[227] And it found that the cellphone location data at issue, which involved Securus "ping[ing]" individuals' cellphones and determining their location based on cell tower signals, was protected under Supreme Court precedent.[228]

Cooper points the way towards a clear-eyed, practical assessment of law enforcement purchases of private data. Specialized data brokers, selling exclusively to law enforcement and offering a product designed for criminal investigations, are essentially working with the police when they obtain private data for law enforcement purposes.[229] The fact that the police purchase the data or surveillance service from them does not change that analysis. To be sure, the location data at issue in *Cooper* was not voluntarily disclosed to cellphone apps, so it remains possible that other types of cellphone data or related services would receive less protection.[230] But, assuming the data is otherwise protected, this early case stands for the principle that purchasing location data does not allow the police to circumvent the Fourth Amendment.[231]

III. DATA COLLECTION AND CONSENT

Government attorneys defending the constitutionality of government purchases of private data have noted that such data is

222. 472 F. Supp. 3d 509 (E.D. Mo. 2020).

223. *Id.* at 512.

224. *Id.*

225. *Id.* at 513. That is, the court so held under the facts alleged by the plaintiff, in the context of evaluating Securus's motion to dismiss.

226. *Id.* at 512.

227. *Id.* at 513 (quoting Adickes v. S.H. Kress & Co., 398 U.S. 144, 151 (1970)).

228. *Id.* at 514 (citing Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018)). The *Cooper* Court found this based on the plaintiffs' pleadings, at the motion to dismiss stage. *Id.* at 512–14.

229. *Id.* at 513; *see supra* note 109–10 and accompanying text.

230. *See infra* Part III.

231. *Cooper*, 472 F. Supp. 3d at 513–14.

often collected via cellphone apps that ask users' permission for data collection.[232] Accordingly, the argument is that these cellphone app users have no reasonable expectation of privacy in their data.[233]

This is a potentially powerful argument: it would largely eliminate data privacy for cellphone users. The overwhelming majority of cellphone users operate apps, virtually all of which collect information and many of which collect detailed location or other personal information.[234] Navigation apps such as Google Maps and Waze, transportation apps like Uber and Lyft, dating apps including Tinder and Hinge, news apps, weather apps, sports apps, social media apps, and countless other apps like flashlight apps and the Angry Birds video game, have collected detailed location information on cellphone users.[235] Most of these apps request permission from users to collect their information before doing so, albeit typically in a cursory form during app set-up.[236] Users typically blindly agree to whatever permissions are required to get the apps operating.[237] Arguably, such agreement constitutes a voluntary disclosure to a third party, sufficient to eliminate any Fourth Amendment rights in user data.

But the idea that consumers waive their Fourth Amendment rights in their data by giving apps permission to collect it may be inconsistent with the realities of modern cellphone use and the Supreme Court's recent curtailment of the third-party doctrine in *Carpenter v. United States*.[238] This Part discusses whether consumers should retain Fourth Amendment rights in their personal data even if they choose to use cellphone apps.

---

232. Tau, *supra* note 15; Treasury Letter, *supra* note 34.

233. Tau, *supra* note 15; Treasury Letter, *supra* note 34.

234. *See, e.g.*, Sara Lebow, *The Top 15 Mobile Apps for US Smartphone App Users*, INSIDER INTEL. (Aug. 12, 2021), http://www.insiderintelligence.com/content/top-15-mobile-apps-us-smartphone-app-users; Joe Parker, *10 Years of Growth of Mobile App Market*, KNOWBAND (July 21, 2022), http://www.knowband.com/blog/mobile-app/growth-of-mobile-app-market

235. *See, e.*g., McAllister, *supra* note 37, at 109; Valentino-DeVries et al., *supra* note 27; BRUCE SCHNEIER, DATA AND GOLIATH: THE HIDDEN BATTLES TO COLLECT YOUR DATA AND CONTROL YOUR WORLD 55–58 (2015); Sidney Fussell, *The Most Important Things to Know About Apps That Track Your Location*, TIME (Sept. 1, 2022, 2:13 PM), http://time.com/6209991/apps-collecting-personal-data; Thomas Germain, *How Private Is Your Online Dating Data?*, CONSUMER REPS. (Sept. 21, 2019), http://www.consumerreports.org/privacy/how-private-is-your-online-dating-data.

236. *See* McAllister, *supra* note 37, at 109.

237. Richards & Hartzog, *supra* note 37, at 1478–79; NPR, *supra* note 37.

238. 138 S. Ct. 2206, 2223 (2018).

A. The Meaninglessness of App Permissions

In contract law, consumers may be bound by adhesion contracts, where contractual terms apply to a customer even if they have not read or understood the terms.[239] But, as the Supreme Court and other courts have indicated, Fourth Amendment law does not turn on contractual terms.[240] For example, an unauthorized driver of a rental car whose use of the car plainly violated the terms of the rental contract nonetheless had Fourth Amendment privacy rights in the car, because contractual rights and Fourth Amendment rights are not coextensive.[241] Likewise, in *Carpenter v. United States*, a cellphone user retained Fourth Amendment rights in cellphone location data despite the absence of any contractual right to control such data.[242]

The same principles should apply in the context of consumer permissions for data collection by apps. While consumers may give apps contractual permission to collect their data, they do not waive their Fourth Amendment rights in such data or consent to police monitoring of their every move.[243]

One problem with the idea that app permissions are sufficient to waive constitutional rights is that app permission screens are typically incomplete or misleading.[244] A typical permission screen might provide a single, generic sentence about how the app will use your location data, such as the Weather Channel app's message: "[You'll] get personalized local weather reports."[245] This screen does not mention that the app will sell your location data to third-party vendors, advertisers, and marketing analysts; does not mention how

---

239. *E.g.*, Aaron E. Ghirardelli, *Rules of Engagement in the Conflict Between Businesses and Consumers in Online Contracts*, 93 OR. L. REV. 719, 723–24 (2015).

240. *See supra* note 35.

241. Byrd v. United States, 138 S. Ct. 1518, 1531 (2018).

242. *See Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting) (discussing the absence of any contractual indication that Carpenter owned the cellphone records in question). Further, in cases like *Quon v. Arch Wireless Operating Co.*, 529 F.3d 892, 896, 898, 906 (9th Cir. 2008), *rev'd on other grounds sub nom. City of Ontario v. Quon*, 560 U.S. 746, 759, 766 (2010) and *United States v. Long*, 64 M.J. 57, 60, 63 (C.A.A.F. 2006), courts have looked beyond the language of Internet policies that provide for total access to employee online data and examined whether employers actually access such data in reality.

243. Theories of contextual integrity and privacy posit that permission granted for information transfers or collection in one context does not necessarily extend to other contexts. *See, e.g.*, Helen Nissenbaum, *Contextual Integrity Up and Down the Data Food Chain*, 20 THEORETICAL INQUIRIES L. 221, 224–34, 252–53 (2019). That is especially applicable in this setting, where information gathered for an anonymous commercial application is used, far downstream, for law enforcement investigation.

244. *See* Valentino-DeVries et al., *supra* note 27; McAllister, *supra* note 37, at 109–10.

245. Valentino-DeVries et al., *supra* note 27.

long your data will be stored; and does not mention how its data may be combined with data from other apps and websites using a variety of tracking technologies.[246] That information is buried deep within a separate privacy policy document that users do not read and likely could not understand.[247] And some uses of information, such as the Weather Channel app's use of location data to analyze foot traffic for commercial purposes, may not be disclosed at all.[248]

Another problem relates to the interaction of humans and complex technologies.[249] Users are often confronted with numerous app permission screens during the initial set-up of their cellphones, and they may be rushed, distracted, and especially prone to just clicking "Accept" and hoping for the best.[250] A single app can ask users for many permissions, with the average app asking for roughly five.[251] The app set-up process may be confusing in general for users who lack technological expertise.[252] Indeed, aside from people working in the advertising technology industry, few users are likely to understand the underlying technologies of location tracking, data storage, third-party data sharing, digital ad networks, targeting algorithms, ad servers, data auctions, and cross-device tracking, to name only a few of the technologies implicated in the collection and processing of consumer cellphone data.[253] The upshot is that most app users have little to no idea about the data collection practices and exposure risks they are accepting when they hit the "Accept" button.[254] Even some advertising industry executives have conceded that "[m]ost people don't know what's going on."[255]

Perhaps a user with hours or days to devote to studying an app's privacy policy and user agreement might be able to glean enough information to learn what that particular app will do with their data. But, to state the obvious, people do not do this. Many users do not

246. *See id.*

247. *Privacy Policy*, THE WEATHER CHANNEL, http://weather.com/en-US/twc/privacy-policy [https://perma.cc/8KU9-7CTR] (last visited Feb. 13, 2024); Valentino-DeVries et al., *supra* note 27; Richards & Hartzog, *supra* note 37, at 1478–86.

248. Valentino-DeVries et al., *supra* note 27 (discussing the Weather App's failure to disclose some commercial applications of its users' data).

249. *See* Richards & Hartzog, *supra* note 37, at 1478–86; Solove, *supra* note 37, at 1883–86.

250. McAllister, *supra* note 37, at 109–10; Richards & Hartzog, *supra* note 37, at 1478.

251. Woodrow Hartzog & Neil Richards, *Privacy's Constitutional Moment and the Limits of Data Protection*, 61 B.C. L. REV. 1687, 1735–36 (2020).

252. *See* McAllister, *supra* note 37, at 110.

253. *See* Richards & Hartzog, *supra* note 37, at 1483–84; Maciej Zawadziński, *What Is an Ad Network and How Does It Work?*, CLEARCODE (June 29, 2023), http://clearcode.cc/blog/what-is-an-ad-network-and-how-does-it-work.

254. Richards & Hartzog, *supra* note 37, at 1479.

255. Valentino-DeVries et al., *supra* note 27.

even understand what a privacy policy is, and many erroneously believe that the mere existence of a privacy policy means that their data will be kept private.[256] Very few people even claim to read privacy policies or user agreements.[257] For example, only 2.9 percent of people reported reading their cellphone company's privacy policy, just one of hundreds of privacy policies that might apply to their data.[258] In reality, the number of people who read their privacy policies or user agreements before agreeing to them is close to zero.[259] In a study that tracked the behavior of software customers online, only 7 out of 4,866 software purchasers (0.14 percent) accessed the user agreement document.[260] Even these 7 customers do not appear to have read the agreement, as the median time spent viewing the document was sixty seconds.[261]

Further, consumers may have good reasons for not reading the many privacy policies that apply to their internet and cellphone use. Privacy policies tend to be written in a mix of legal terms and technological terms that the average consumer is unlikely to understand.[262] Some privacy policies are so vague, or so confusingly or poorly written, that no reader could understand all of their terms.[263] Another obstacle is the sheer length and volume of all of the privacy policies and user agreements that apply to a cellphone or internet user. Virtually all of the apps and websites a user encounters have lengthy privacy policies and terms of use agreements that stretch on for many pages, like Apple's 55-page iTunes contract.[264] A 2008 study calculated that each internet user would have to dedicate 244 hours annually to read all of their privacy policies.[265] This number would surely be far greater today, when so much more of daily life is conducted via the internet and smartphone.

Nor would fully reading and comprehending privacy policies do most consumers much good. Consumer data collected for marketing

---

256. Tokson, *supra* note 68, at 175.

257. *See, e.g.*, Joseph Turow et al., *The Federal Trade Commission and Consumer Privacy in the Coming Decade*, 3 I/S: J.L. & POL'Y FOR INFO. SOC'Y 723, 740 (2007–08) (only 1.4 percent of poll respondents reported reading their user agreements more than rarely).

258. Tokson, *supra* note 68, at 178–79.

259. *See* Yannis Bakos, Florencia Marotta-Wurgler & David R. Trossen, *Does Anyone Read the Fine Print? Consumer Attention to Standard-Form Contracts*, 43 J. LEGAL STUD. 1, 20 (2014).

260. *Id.*

261. *Id.* The average time spent viewing the user agreement was less than three minutes. *Id.*

262. Richards & Hartzog, *supra* note 37, at 1479–80.

263. *Id.*

264. NPR, *supra* note 37.

265. McDonald & Cranor, *supra* note 38, at 564–65. This calculation does not appear to include user agreement documents, which are often separate from privacy policies.

purposes tends to be stored in large, anonymized blocks of data processed by automated ad servers.[266] Although this data can often be deanonymized, ad company employees are unlikely to individually stalk their customers, and the data is likely to remain unlinked to individual users unless a police officer takes the time to deanonymize it.[267] Consumers generally perceive the capture of anonymous data as substantially less worrisome than that of personal information.[268] Likewise, consumers are generally far less worried about the disclosure of their information to automated systems than to other humans.[269] A user who permits anonymized, automated data processing does not also agree to being deanonymized and tracked by government agents; the two things are qualitatively different.

Accordingly, consumers do not consent to police tracking of their personalized data when they give apps permission to use their data. Users are largely unaware of how the apps collect and store and market their data; they do not read the applicable privacy policies and could not feasibly do so even if they tried; and the anonymized and automated processing of their information by private companies in no way resembles the personalized, human observation involved in police surveillance.[270]

---

266. *See* Tokson, *supra* note 27, at 602–09.

267. *See* Valentino-DeVries et al., *supra* note 27; Tokson, *supra* note 27, at 604–09.

268. Christopher Slobogin, *Government Data Mining and the Fourth Amendment*, 75 U. CHI. L. REV. 317, 335 tbl. (2008) (poll respondents rated anonymous record gathering less intrusive than non-anonymous record gathering).

269. Tokson, *supra* note 27, at 619–29.

270. It is commendable that Android and iOS have taken steps to encourage users to limit location data disclosures to only when a given app is in use. *See* Suchi Bansal, *Android 12 Privacy Changes for Location*, PROANDROIDDEV (June 22, 2021), http://proandroiddev.com/android-12-privacy-changes-for-location-55ffd8c016fd; Sachin Srivastava, *iOS 14+ Privacy Through Location Permissions*, MEDIUM (Jul 15, 2021), http://medium.com/microsoft-mobile-engineering/ios-14-privacy-through-location-permissions-c73eaa382547. This generally does not apply to all apps, including widely used apps like Google or built-in apps designed by phone manufacturers. *See infra* Subpart III.B. Users may also affirmatively use apps like weather apps, voice assistant apps, transportation and navigation apps, dating apps, and many others frequently enough that their location data is thoroughly tracked even if they are diligent about limiting permissions. The latest mobile operating systems also provide users with an option to use less precise location data, although doing so is likely to decrease the usefulness of many location-based apps, and switching to imprecise data typically requires the user to affirmatively opt out of precision data, an extra step that users are unlikely to expend the effort to take. *See* Bansal, *supra*; Srivastava, *supra*. *See generally* Matthew Tokson, *Judicial Resistance and Legal Change*, 82 U. CHI. L. REV. 901, 914 (2015) (discussing people's tendency to stick with default choices).

B. Automatic Disclosure

In *Carpenter v. United States*, the Supreme Court determined that the third-party doctrine should not apply to cellphone tracking in part because cellphone data was transmitted automatically, rather than by some affirmative act by the cellphone user.[271] Virtually any user activity, such as "checking for news, weather, or social media updates," automatically generated location data.[272] Indeed, such data was generated whenever a cellphone was operating.[273]

Some lower courts applying *Carpenter* have looked to whether a user automatically discloses their information as a basis for granting or denying Fourth Amendment protection.[274] Certain courts, typically those that seek to preserve a stringent third-party doctrine and to interpret *Carpenter* as narrowly as possible, have focused heavily on this factor.[275] Others consider automatic disclosure as only one factor of several in a *Carpenter* inquiry or ignore it altogether.[276]

In any event, much of the disclosure of location and other information to cellphone apps is automatic, occurring without any affirmative act by the user. Apps that continually monitor a user's location do so constantly, even when the app is turned off.[277] Other apps may only collect location data while "in use," but that term refers not just to when a person is actively using an app but also when the app is in the background of the phone, not being used.[278] To be sure, some of these apps may be automatically deactivated by a phone's operating system, but others are allowed to run in the background persistently.[279]

In some cases, users do actively disclose their data to a cellphone app, such as when a person orders an Uber and shares their location so they can be picked up. But most cellphone data disclosures do not work this way. Consumers do not waive their Fourth Amendment rights when cellphone apps automatically collect their data without any affirmative act on their part.[280] A database of information about

---

271. Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

272. *Id.*

273. *Id.*

274. Tokson, *supra* note 43, at 1823.

275. *See id.*

276. *See id.*; Tokson, *supra* note 56, at 519–20.

277. *See, e.g.*, McAllister, *supra* note 37, at 109; Valentino-DeVries et al., *supra* note 27.

278. *See, e.g.*, *About Privacy and Location Services in iOS and iPadOS*, APPLE SUPPORT, http://support.apple.com/en-us/HT203033 (last visited Feb. 13, 2024).

279. *See, e.g.*, *Change App Permissions on Your Android Phone*, ANDROID HELP, https://support.google.com/android/answer/9431959?sjid=2406360024405824911-NA#zippy=%2Cautomatically-remove-permissions-for-unused-apps (last visited Feb. 13, 2024).

280. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018).

a cellphone user, much of which has been collected automatically, is likely to be off limits to warrantless acquisition under *Carpenter*.[281]

C. Inescapability

The Supreme Court's *Carpenter* opinion also found that cellphone location data was not voluntarily disclosed to a third party because cellphone use is "inescapable" in modern life.[282] In other words, users have no real choice but to use cellphones if they wish to live normal lives.[283] Roughly 97 percent of Americans currently own a cellphone of some kind.[284]

Cellphone apps are, in theory, more avoidable than cellphones themselves. Apps are most widely used in smartphones, which only about 85 percent of Americans own.[285] And any particular app is optional for smartphone users; they can do without it or use another, competing app. But for the hundreds of millions of American smartphone owners, the use of one app or another is virtually inevitable. Industry analysts estimate that the average American has 80 apps on their phone and that roughly 85 percent of all time spent on smartphones is spent using apps.[286] And apps, including the most popular apps, tend to aggressively collect user data.[287] To use a smartphone, as the vast majority of Americans do, is to use apps that collect one's personal data. Such data collection is not significantly more escapable than cellphone use itself.

In theory, users can opt out of information tracking by denying their apps permission to collect location or other data.[288] But the result of denying permission is often that the app will not work, or at

---

281. That is, it is likely to be off limits unless the police can separate out the automatically disclosed information from the voluntarily disclosed information. In any event, construing *Carpenter* to withhold Fourth Amendment protection from *all* voluntarily disclosed information would be to ignore the vast majority of the *Carpenter* opinion, which focuses largely on the revealing nature and amount of the data captured, not the voluntariness of the disclosure. *See id.* at 2217–19; *infra* Subpart III.D.

282. *Carpenter*, 138 S. Ct. at 2223.

283. *See id.*

284. *Mobile Fact Sheet*, PEW RSCH. CTR. (Apr. 7, 2021), http://www.pewresearch.org/internet/fact-sheet/mobile.

285. *Id.*

286. *See* Jack Flynn, *40 Fascinating Mobile App Industry Statistics [2023]: the Success of Mobile Apps in the U.S.*, ZIPPIA (Oct. 19, 2022), http://www.zippia.com/advice/mobile-app-industry-statistics.

287. *See, e.g.*, David Curry, *Most Popular Apps (2023)*, BUS. OF APPS (Feb. 28, 2023), http://www.businessofapps.com/data/most-popular-apps; Asha Barbaschow, *Turns Out TikTok Does Have an Alarming Level of Access to Your Phone*, GIZMODO AU (July 18, 2022, 12:34 PM), http://www.gizmodo.com.au/2022/07/tiktok-app-phone-access.

288. *See, e.g.*, McAllister, *supra* note 37, at 110.

least will not function in any useful way.[289] The choice between permitting data collection or having useless apps is not a meaningful choice, nor one that can provide a basis for Fourth Amendment waiver. And in some cases, users are not even given this pseudo-choice. For example, on a Samsung S21 smartphone running Android, at least two pre-loaded apps collect location data on users all of the time, even when the apps are switched off entirely: Google Search and Bixby Voice (Samsung's voice assistant app). Users can only deny these apps permission if they access the cellphone's location permission settings and manually adjust the setting. But even users who attempt to manually deny permission will receive the following message: "If you deny this permission, basic features of your device may no longer work as intended."[290] Obviously, the choice between granting data collection permission and having one's cellphone cease to function is no choice at all. The data collection, in other words, is inescapable. In other contexts, Google has been sued for collecting location information from users who specifically denied permission for such collection, suggesting that data collection is sometimes inescapable even for those who believe they have been given a choice to escape it.[291]

More broadly, the fluidity and vagueness of the inescapability analysis should lead courts to doubt its usefulness. The use of one app might be considered escapable, while the use of apps in general might be considered inescapable, and there is little guidance in *Carpenter* for courts attempting to apply this concept.[292] Moreover, the inescapabilty analysis threatens to punish people for using helpful apps such as Uber, Google Search, Google Maps, dating apps, social media apps, and weather apps, as well as countless other services and websites accessible from a cellphone. These services are each in theory voluntary and avoidable, but in practice a beneficial and important part of modern life.[293] Navigation apps reduce traffic and help users avoid getting lost;[294] dating apps lead to millions of marriages and relationships and are especially important to LGBTQ+ communities;[295] ride-sharing app use is correlated with a significant

289. *See, e.g.*, *id.*

290. Screen captures of this message are on file with the author.

291. Cecilia Kang, *Four Attorneys General Claim Google Secretly Tracked People*, N.Y. TIMES (Jan. 24, 2022), http://www.nytimes.com/2022/01/24/technology/google-location-services-lawsuit.html.

292. *See* Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018) (mentioning inescapability in only a single sentence in the analysis portion of the opinion).

293. Tokson, *supra* note 44, at 433–37.

294. *Id.* at 434.

295. *Id.* at 435–36; Anna Brown, *Couples Who Meet Online Are More Diverse than Those Who Meet in Other Ways, Largely Because They're Younger*, PEW RSCH. CTR. (June 24, 2019), http://www.pewresearch.org/fact-tank/2019/06/24/couples-who-meet-

reduction in drunk driving deaths.[296] Penalizing users for disclosing their data to service providers creates perverse incentives and is incompatible with meaningful Fourth Amendment protection in the digital age. In addition, it can create substantial inequalities in Fourth Amendment law. Technologies that are avoidable for most people are often unavoidable for others, including people with disabilities, people in poverty, and other disadvantaged populations.[297]

D. Additional Carpenter Factors

The Supreme Court's *Carpenter* opinion discussed, in addition to automatic disclosure and inescapability, several other factors that drove its decision.[298] Most of those factors likewise indicate that information disclosed to cellphone apps remains protected by the Fourth Amendment.

As the Court concluded, location data associated with a cellphone is "deeply revealing" because it "provides an all-encompassing record of the holder's whereabouts."[299] Knowing everywhere that a person goes gives the government "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.'"[300] Cellphone app location data is often more precise than the data at issue in *Carpenter*, because it relies primarily on GPS data or Wi-Fi location tracking rather than cell tower signals.[301] Its potential for

online-are-more-diverse-than-those-who-meet-in-other-ways-largely-because-theyre-younger.

296. Jacey Fortin, *Does Uber Really Prevent Drunken Driving? It Depends on the Study*, N.Y. TIMES (Apr. 7, 2017), http://www.nytimes.com/2017/04/07/business/uber-drunk-driving-prevention.html (noting that studies predominantly show a correlation between Uber services and lower rates of alcohol-related accidents).

297. Tokson, *supra* note 44, at 409.

298. Carpenter v. United States, 138 S. Ct. 2206, 2217–19 (2018).

299. *Id.* at 2217.

300. *Id.* (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

301. *See id.* at 2218; GPS tracking is often assisted by cell site location data in order to save cellphone battery power. *See, e.g.*, Jerry Hildenbrand, *How Does GPS Work on My Phone?*, ANDROIDCENTRAL (Nov. 10, 2020), http://www.androidcentral.com/how-does-gps-work-my-phone; Theodor Perutiu, *Wi-Fi Location Tracking, How Does It Work?*, VPNOVERVIEW (Mar. 17, 2022), http://vpnoverview.com/privacy/devices/wi-fi-location-tracking; Justin Scheck, *Stalkers Exploit Cellphone GPS*, WALL ST. J. (Aug. 4, 2010), https://www.wsj.com/articles/SB10001424052748703467304575383522318244234; Valentino-DeVries et al., *supra* note 27.

revealing the intimate details of a user's life is even greater than that of cell site location information.[302]

The *Carpenter* Court also addressed the remarkable amount of data collected via cellphone signal tracking, which captured over 100 data points each day and could stretch back up to five years into the past.[303] These massive quantities of data enabled to government to pervasively track an individual's location and substantially increased the potential for serious privacy intrusions.[304] Even seven days of cellphone signal tracking produced so much data as to constitute a Fourth Amendment search.[305] Cellphone app location data may be even more voluminous, often including far more than 100 data points per day and stretching back for as many years as apps and data marketers choose to store it.[306] The amount of location data captured by apps may pose an even greater privacy risk than the CSLI data at issue in *Carpenter*. Other factors mentioned in *Carpenter*, although less influential in the lower courts,[307] similarly tend to indicate that

---

302. *Cf. Carpenter*, 138 S. Ct. at 2217 (discussing the revealing nature of CSLI).

303. *Id.* at 2212, 2218.

304. *Id.* at 2218–20 (noting the dangers to privacy of "a detailed chronicle of a person's physical presence compiled every day, every moment, over several years [because s]uch a chronicle implicates privacy concerns far beyond those considered in [previous third-party doctrine cases]"); Matthew Tokson, *The Emerging Principles of Fourth Amendment Privacy*, 88 GEO. WASH. L. REV. 1, 18 (2020) (discussing the privacy threats posed by large collections of data).

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

306. *See* Valentino-DeVries et al., *supra* note 27 (describing a database containing information on user locations from a year prior, accurate to within a few yards, and containing up to 14,000 per day on some users); *see also id.* (noting that some tracking companies "keep the information for years"); Joe Keegan & Alfred Ng, *There's a Multibillion-Dollar Market for Your Phone's Location Data*, MARKUP (Sept. 30, 2021, 3:51 PM), http://themarkup.org/privacy/2021/09/30/theres-a-multibillion-dollar-market-for-your-phones-location-data (noting that one data broker advertised "5+ Years of Data").

307. Tokson, *supra* note 56, at 510. The *Carpenter* opinion discussed the low cost of cellphone location tracking, and some lower courts have analyzed cost when applying *Carpenter*. *Carpenter*, 138 S. Ct. at 2217–18. Tokson, *supra* note 76, at 999–1000. Low-cost surveillance often operates with little oversight and may be overused or abused, while high-cost surveillance tends to be more visible and more limited. Tokson, *supra* note 304, at 24; *see also* United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring) (internal quotation marks omitted) (contending that GPS tracking was so "cheap in comparison to conventional surveillance techniques" that it would evade "the ordinary checks that constrain abusive law enforcement practices: limited police resources and community hostility"). The price of a license to access consumer location data is substantial, ranging from $7,500 per year for a police department to $100,000 or more for a federal government agency like the Department of Homeland Security. Burke & Dearen, *supra* note 8; *Delivery Order (DO) PIID HSHQDC17J00525, Department of Homeland Security and Panamerica Computers, Inc.*,

the Fourth Amendment's protection extends to data disclosed to cellphone apps.[308]

IV. IMPLICATIONS AND SOLUTIONS

A. The Inadequacy of Consumer Privacy Law

The broader issue of government purchases of private data arises because of the lack of effective consumer privacy regulation in the United States. The collection, sale, and processing of sensitive data is hardly regulated at all in the United States, outside of a few unique areas such as health and education.[309] This lack of regulation threatens consumer privacy, as private companies amass increasingly detailed dossiers on people's lives and associations.[310]

The United States lacks a comprehensive privacy statute, and its privacy law is a complex patchwork of piecemeal federal laws, state statutes, regulatory rulings, and contract and tort law.[311] Outside of a few narrow areas, its approach to data privacy regulation is permissive, allowing companies to use consumer data for virtually any purpose so long as they disclose those uses in a privacy policy or

---

USASPENDING (Sept. 29, 2017), http://www.usaspending.gov/award/CONT_AWD_HSHQDC17J00525_7001_HSHQDC12D00013_7001. However, this price grants government entities potential access to any of hundreds of millions of cellphones, permitting them to track the location of nearly anyone they choose, even if their total number of searches may be limited by some of the cheaper licenses. *See, e.g.*, Burke & Dearen, *supra* note 8. The cost per search of such tracking may be relatively low, depending on how often the government uses the technology. The price structure of location data purchasing may also encourage overuse and abuse of the technology.

308. *See supra* note 299–300 and accompanying text. The *Carpenter* opinion also referenced the number of people potentially affected by cellphone location tracking, noting that "because location information is continually logged for all of the 400 million [cellular] devices in the United States . . . this newfound tracking capacity runs against everyone." *Carpenter*, 138 S. Ct. at 2218. Lower courts have largely ignored, or outright rejected, the idea that the number of people affected should be a factor in post-*Carpenter* Fourth Amendment analyses. Tokson, *supra* note 43, at 1824. Were this factor to matter in applying *Carpenter* to government purchases of cellphone location data, it would weigh heavily towards finding such purchases to be a Fourth Amendment search. By accessing a tracking company's vast databases of cellphone location data, a police department would potentially be able to track any of hundreds of millions of Americans. *See* Burke & Dearen, *supra* note 8 (referring to one service's ability to search "hundreds of billions of data points from 250 million mobile devices").

309. *See, e.g.*, Hartzog & Richards, *supra* note 251, at 1704 (noting that the Health Insurance Portability and Accountability Act and Family Educational Rights and Privacy Act have more requirements than general federal privacy law).

310. *E.g.*, CITRON, *supra* note 146, at 3–23.

311. *See, e.g.*, Hartzog & Richards, *supra* note 251, at 1697.

other document.[312] This "notice and choice" regime places a heavy burden on consumers to discover and respond to invasive data processing.[313] Notice, in this context, does not refer to actual notice but to publication in a privacy policy document that goes unread by virtually all users.[314] Nor do companies typically disclose anything about the parties to whom they sell or the potential for subsequent downstream sales to law enforcement.[315] And consumer choice is generally limited to either accepting a company's data collection practices or going without whatever service they provide.[316] So long as companies do not engage in unfair or deceptive trade practices when collecting and processing data, which would generally entail lying about their practices or egregiously failing to disclose them, United States regulators will not interfere.[317] Companies can collect, use, and sell even the most intimate personal data if they avoid flagrant violations of these norms.[318]

In practice, companies collect vast quantities of personal data, much of it even more revealing than location data.[319] This includes web site visits, search queries, IP address data, dating app profiles and activities, health data, pornography sites and searches, Facebook likes and posts, online purchases, mental health app data, menstrual cycle and pregnancy data, and data culled from a variety of smart devices such as Amazon's Alexa.[320] This data is processed and sold by a variety of data brokers and their customers, largely in order to market goods and services to consumers.[321] Purchasing companies may also use this information to facilitate algorithmic decision-making, particularly in the insurance, health, and employment contexts.[322] The websites a user visits and the apps they use may be leveraged to deny them a job, raise their insurance premiums, and more.[323]

---

312. *E.g.*, *id.* at 1690, 1704; *see also* Richards & Hartzog, *supra* note 45, at 444 (explaining that companies can act "in any way consistent with the notice given to consumers").

313. Richards & Hartzog, *supra* note 45, at 444.

314. *Id.*

315. *See* Keegan & Ng, *supra* note 306 (discussing how many apps sell consumers' location data to other companies without the knowledge of consumers, and that it may go to law enforcement or political agencies down the line).

316. Hartzog & Richards, *supra* note 251, at 1704.

317. CITRON, *supra* note 146, at 98.

318. *Id.*

319. *Id.* at 9.

320. *See id.* at 9–10; Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 559 (2017).

321. *See* CITRON, *supra* note 146, at 13.

322. *Id.* at 19–21.

323. *Id.* at 20–21.

Yet purchases of intimate data by law enforcement agents are perhaps the most intrusive use of consumer information in our unregulated data environment. Law enforcement officers are not engaged in marketing or premium setting; their goal is to monitor citizens and potentially build a criminal case against suspects. The tendency of law enforcement to use surveillance powers overzealously is well documented.[324] Perhaps even more concerning is the possibility for abuses having little to do with law enforcement goals, including officers tracking individuals for personal reasons or surveilling reporters and activists for political purposes.[325] Poorly regulated markets in intimate data present the government with an opportunity to surveil its people at unprecedented levels.

B. Surveillance Interoperability

The potential uses and abuses of data purchased by law enforcement vary with the type of data. Location data can be used for a variety of law enforcement purposes: to check suspects' alibis, identify persons near the scene of a crime, build detailed profiles of suspects' lives, monitor activists or protestors, track movement near borders, locate undocumented immigrants, and more.[326] Web-surfing data can link suspects to crimes committed on-or-offline or identify people who read a certain article or visit protest-affiliated websites.[327] Smart appliances and devices can give police the ability to surveil activity inside the home.[328] Smart pacemakers and medical devices can produce digital evidence against their users.[329]

Data from "femtech" apps that help women manage birth control, pregnancy, and menstruation may be used to monitor women who might otherwise obtain abortions in jurisdictions where abortion is unlawful.[330] This could be supplemented with location data, web-surfing data, or web search data that might further reveal abortion-

---

324. *See, e.g.*, Tokson, *supra* note 27, at 583–84; ALEXANDER CHARNS, CLOAK AND GAVEL: FBI WIRETAPS, BUGS, INFORMERS, AND THE SUPREME COURT 17–20, 52 (1992).

325. *See supra* note 21.

326. *See supra* notes 1–12, 96–97, 107, 111–13 and accompanying text.

327. *See, e.g.*, United States v. Gratkowski, 964 F.3d 307, 309 (5th Cir. 2020) (addressing website and Bitcoin evidence used in a child pornography investigation); United States v. Forrester, 512 F.3d 500, 505–06 (9th Cir. 2008) (addressing website evidence used in a drug lab investigation); Colin Lecher, *The Justice Department is Demanding Information on Visitors to an Anti-Trump Website*, VERGE (Aug. 14, 2017, 4:42 PM), http://www.theverge.com/2017/8/14/16145812/justice-department-disruptj20-trump-website-warrant; Politi, *supra* note 48.

328. *See* Matthew Tokson, *The Next Wave of Fourth Amendment Challenges After* Carpenter, 59 WASHBURN L.J. 1, 15 (2020).

329. *See id.* at 15–16.

330. CITRON, *supra* note 146, at 15.

related activities.[331] This data may be commercially available, and government entities have already shown an interest in acquiring it.[332] For instance, during the Trump Administration, the Office of Refugee Resettlement collected data on asylum-seeking minors' menstrual cycles and pregnancies in order to track their potential for seeking abortions.[333] Similar data might be used to enforce discriminatory laws prohibiting doctors from giving gender-affirming care to transgender minors, such as those passed recently in Alabama, Arizona, Tennessee, South Dakota, and Utah,[334] and proposed in several other states.[335] Transgender adults may also be targeted by discriminatory laws via purchases of intimate, commercially available data.[336]

The ability of the government to monitor individuals with purchased data currently extends to any form of data that private companies collect—and tech companies collect virtually every piece of information available about their users.[337] Consumers' lack of privacy vis-à-vis commercial entities has started to bleed over into a lack of privacy against personalized government monitoring. This slippage from private to government surveillance resembles a phenomenon known as "surveillance interoperability"—when government monitoring technologies are leveraged by private firms

331. *See* Cox, *supra* note 152; Danielle Keats Citron, *Intimate Privacy in a Post*-Roe *World*, FLA. L. REV. (forthcoming 2024).

332. *See* CITRON, *supra* note 146, at 14–17, 62–63; Laura Vozzella & Gregory S. Schneider, *Youngkin Opposes Effort to Shield Menstrual Data from Law Enforcement*, WASH. POST (Feb. 14, 2023), http://www.washingtonpost.com/dc-md-va/2023/02/14/youngkin-menstrual-data-abortion-virginia; Anisha Kohli, *Florida May Force High School Athletes to Disclose Their Menstrual History*, TIME (Feb. 1, 2023, 5:39 PM), http://time.com/6252147/florida_student_athletes_menstrual_history.

333. CITRON, *supra* note 146, at 62–63.

334. *See* Alabama Vulnerable Child Compassion and Protection Act, ALA. CODE § 26-26-4 (2022); ARIZ. REV. STAT. ANN. § 32-3230 (2023); Youth Health Protection Act, TENN. CODE ANN. § 63-1-803 (2023); H.R. 1080, 98th Legis. Sess. (S.D. 2023); S. 0016, 2023 Gen. Sess. (Utah 2023).

335. *See, e.g.*, Legis. B. 574, 108th Legis., 1st Sess. (Neb. 2023); S. 12, 2023 Legis. Sess. (Kan. 2023); H. 1011, 59th Legis. (Okla. 2023); H. 619, 168th Legis. Sess. (N.H. 2023); H. 456, 2023 Reg. Sess. (Miss. 2023); S. 164, 102nd Gen. Assemb., 1st Reg. Sess. (Mo. 2023); H. 42, 88th Legis., Reg. Sess. (Tex. 2023).

336. Laws targeting adult transgender women in collegiate sports include Fairness in Women's Sports Act, IDAHO CODE § 33-6201 (2020); Fairness in Women's Sports Act, FLA. STAT. § 1006.205 (2021); Save Women's Sports Act, MONT. CODE ANN. § 20-7-1306 (2021); Save Women's Sports Act, S.C. CODE ANN. § 59-1-500 (2022). Proposed laws targeting transgender adults include S. 12, 2023 Legis. Sess. (Kan. 2023) (proposing to bar gender-affirming care to adults under 21); S. 129, 59th Legis., 1st Sess. (Okla. 2023) (proposing to bar gender-affirming care to adults under 26).

337. *See supra* notes 320–21 and accompanying text.

to track their workers or customers—but in reverse.[338] Because commercial data collection and monitoring is so extensive and unregulated, government entities can achieve near-pervasive surveillance by piggybacking on it.[339] Private surveillance is interoperable with law enforcement surveillance, mediated by competitive markets in private data. The question remains whether these types of surveillance are legally interoperable: whether the legality of private data collection will erode existing constitutional protections against government monitoring.[340] The following sections examine a variety of ways that legal actors can prevent private data markets from undermining Fourth Amendment rights.

C. Potential Solutions

1. Jurisprudential

This Article contends that government purchases of protected private data violate the Fourth Amendment. Courts should exclude from trial any evidence obtained via the purchase of sensitive data and permit lawsuits under Section 1983 or other causes of action for the violation of plaintiffs' constitutional rights.[341] Judicial remedies like these have several advantages. They are relatively nimble, as surveillance targets can seek relief as soon as they discover they have been tracked.[342] They provide a constitutional floor, establishing limits on police activity even where legislatures are hesitant to check police excesses.[343] In the many policy areas where legislation has been slow or nonexistent, judicial rulings can effectively regulate harmful police behavior.[344]

However, the unique context of market-based surveillance presents challenges for effective judicial regulation. Many private companies have gone to great lengths to insulate government purchases from judicial scrutiny, contractually prohibiting law enforcement from mentioning their tracking services in any public

338. *See* Karen Levy, *Labor Under Many Eyes: Tracking the Long-Haul Trucker*, LPE PROJECT (Jan. 21, 2023), http://lpeproject.org/blog/labor-under-many-eyes.

339. *See supra* Subpart I.C.

340. *See* KAREN LEVY, DATA DRIVEN: TRUCKERS, TECHNOLOGY, AND THE NEW WORKPLACE SURVEILLANCE 74–75 (2023).

341. *See* 42 U.S.C. § 1983; Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388 (1971); Cooper v. Hutcheson, 472 F. Supp. 3d 509, 514 (E.D. Mo. 2020).

342. *Cf.* Tokson, *supra* note 68, at 193 (discussing the relative slowness of legislation, particularly in the Fourth Amendment context).

343. Barry Friedman, *Lawless Surveillance*, 97 N.Y.U. L. REV. 1143, 1200 (2022); Matthew Tokson, *The Normative Fourth Amendment*, 104 MINN. L. REV. 741, 797–98 (2019).

344. *See* Friedman, *supra* note 343, at 1200–03.

record.[345] Given the questionable legality of purchasing protected data, law enforcement officials may also be motivated to avoid mentioning such purchases in court. They tend to use this data to generate leads and additional evidence rather than introducing it directly.[346] As a result, purchased data only rarely appears in court documents.[347] Surveillance targets often will not know that they have been tracked via purchased private data; they will either be surveilled without arrest or be searched or arrested on pretextual grounds.[348] A suspect cannot sue a police department for purchasing their data if they never find out about the purchase.

Government data purchases intentionally kept out of public records are an extreme example of a larger phenomenon of government surveillance practices that are not transparent to their targets or the public.[349] Similar issues arise in contexts like national security, where officials sometimes engage in "parallel construction"—when law enforcement intentionally obscures where evidence came from in order to avoid judicial review of a surveillance practice.[350] Police may attempt to launder potentially unlawful surveillance by recreating information obtained via invasive digital searches though more traditional and lawful means.[351] The secrecy of such practices impedes efforts to rein in excessive or abusive surveillance.[352]

Bringing these practices to light, and exposing them to potential civil rights litigation, may first require successful transparency litigation to compel the disclosure of government records.[353] Public interest organizations, public defenders' offices, or individuals can sue government entities under FOIA or its state equivalents, seeking

345. *See supra* notes 1, 105.

346. *See supra* notes 120–22, 139–42 and accompanying text.

347. *See, e.g.*, Cooper v. Hutcheson, No. 1:17 CV 73 ACL, 2017 WL 4404457, at *2 (E.D. Mo. Oct. 4, 2017) (discussing the prior use of purchased location data in a criminal case).

348. *See* Patrick Toomey & Brett Max Kaufman, *The Notice Paradox: Secret Surveillance, Criminal Defendants, & the Right to Notice*, 54 SANTA CLARA L. REV. 843, 863–64 (2015).

349. *See* Hannah Bloch-Wehba, *Visible Policing: Technology, Transparency, and Democratic Control*, 109 CAL. L. REV. 917, 920–21 (2021); Toomey & Kaufman, *supra* note 348, at 848.

350. *See* Toomey & Kaufman, *supra* note 348, at 863–64 (describing how officers may make a given piece of evidence appear as if it came from a certain source when it originally came from a different source, such as NSA surveillance).

351. *Id.*; Bloch-Wehba, *supra* note 349, at 958.

352. Bloch-Wehba, *supra* note 349, at 921–22.

353. *Id.* at 922; *see also* Natalie Ram, *Innovating Criminal Justice*, 112 NW. UNIV. L. REV. 659, 689–90 (discussing transparency benefits in the context of criminal justice technology).

records relevant to purchases of sensitive data.[354] Federal transparency laws like those requiring public disclosure of information about most federal government contracts with private companies also offer some insight into government purchases of data, although the contracts themselves are typically not disclosed.[355] Disclosures obtained via discovery or court orders in civil litigation and subpoenas issued by government agencies investigating police misconduct can also be fruitful sources of police records on surveillance practices.[356] Whatever form it takes, transparency litigation will often be a necessary precursor to effective civil rights litigation targeting unlawful government purchases of protected data.[357]

Alternatively, courts might hold that the Fourth Amendment or Due Process requires notice to defendants of all the searches that led to the introduction of evidence against them, not just the most recent search.[358] For instance, if the police purchase a suspect's private data and then use that data to search the suspect when they know he possesses cocaine, the police would have to disclose the initial purchase.[359] Because defendants have a Fourth Amendment right to challenge subsequent searches as the "fruit of the poisonous tree" of an earlier unlawful search, it arguably follows that they must receive

---

354. *See, e.g.*, Bloch-Wehba, *supra* note 349, at 928–30; Freedom of Information Act, 5 U.S.C. § 552 (2007); Freedom of Information Law, N.Y. PUB. OFF. LAW § 87 (McKinney 2023).

355. *See* Digital Accountability and Transparency Act of 2014 (DATA Act), Pub. L. No. 113-101, 128 Stat. 1146; Sean Moulton, *Contract Transparency: What Uncle Sam Can Learn from the States*, POGO (Mar. 15, 2017), https://www.pogo.org/analysis/contract-transparency-what-uncle-sam-can-learn-from-states ("[C]ontracts and other documents are not among the information [the] federal government is required to make available through the site, and agencies appear unwilling to voluntarily take up the task.").

356. Bloch-Wehba, *supra* note 349, at 945–46; Daniels v. City of New York, 200 F.R.D. 205, 207 (S.D.N.Y. 2001) (discussing the NYPD's disclosure of stop-and-frisk reports to federal investigators); Daniels v. City of New York, No. 99 Civ. 1695(SAS), 2008 WL 2077150, at *1 (S.D.N.Y. July 16, 2007) (detailing an agreement in a civil suit that the NYPD would disclose its stop-and-frisk records to plaintiffs challenging its programs); *see also* Rebecca Wexler, *Privacy Asymmetries: Access to Data in Criminal Defense Investigations*, 68 UCLA L. REV. 212, 215–17 (2021) (discussing difficulties that some privacy statutes pose for criminal defendants seeking discovery of electronic data).

357. *See* Brennan Ctr. for Just. v. New York City Police Dep't, No. 160541/2016, 2017 WL 6610414, at *2–3 (N.Y. Sup. Ct. Dec. 27, 2017) (seeking purchase records, contracts, and other records relating to New York's purchase of surveillance programs from a private company).

358. Toomey & Kauffman, *supra* note 348, at 862–64.

359. *Cf.* Tau & Hackman, *supra* note 1; Martinez, *supra* note 7 (describing how police used purchased data to pretextually pull over a drug-trafficking suspect over for an "equipment violation").

notice of the earlier search.[360] Courts have not yet expressly identified such a right, although this may be because digital data searches without notice are relatively new and, by their nature, obscure.[361] Recognizing a right to notice of all relevant searches conducted in a criminal investigation would facilitate judicial oversight of government data purchases.

2. Statutory

There are many potential legislative solutions to the problem of government purchases of sensitive private data. They range from narrowly targeted prohibitions on data purchases to more comprehensive consumer privacy regimes.

Legislatures could directly prohibit government entities from purchasing specific types of data, such as location data. They could ban virtually all government purchases of customer records, as the proposed Fourth Amendment Is Not For Sale Act would do.[362] Or they could ban all purchases of location data by any entity, as would a proposed Massachusetts law.[363] They might alternatively prohibit the purchase of any data deemed constitutionally protected under current law. That last approach may fail to effectively protect user privacy, however, as the Supreme Court rarely weighs in on new forms of data until years or decades after their first uses.[364] Police would likely be able to claim that the form of data they are purchasing has not been unambiguously protected under current law, even if it is closely analogous to protected information.[365]

Legislatures might instead adopt more comprehensive consumer privacy regulations that shrink or transform existing markets in

---

360. *See* Murray v. United States, 487 U.S. 533, 536–37 (1988); Wong Sun v. United States, 371 U.S. 471, 484–85 (1963); Toomey & Kauffman, *supra* note 348, at 863–64; Jesse Lieberfeld & Neil Richards, *Fourth Amendment Notice in the Cloud*, 103 B.U. L. REV. 1201, 1241 (2023).

361. *See* Toomey & Kauffman, *supra* note 348, at 847; *see also* Bloch-Wehba, *supra* note 349, at 934 (discussing the notice associated with traditional physical searches); *cf.* United States v. United States Dist. Ct. for the E. Dist. of Mich., S. Div., 407 U.S. 297, 336 (1972) (White, J., concurring in the judgment) (noting that a lower court had ordered the Government to disclose to defendants records of their wiretapped conversations in a national security investigation after holding that the wiretap violated the defendant's Fourth Amendment rights).

362. *See* Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021).

363. *See* Byron Tau, *Selling Your Cellphone Location Data Might Soon Be Banned in U.S. for First Time*, WALL ST. J. (July 10, 2023), http://www.wsj.com/articles/first-u-s-ban-on-sale-of-cellphone-location-data-might-be-coming-fbe47e53.

364. Matthew Tokson & Ari Ezra Waldman, *Social Norms in Fourth Amendment Law*, 120 MICH. L. REV. 265, 267–68 (2021).

365. For example, government attorneys have argued that app-based location data is not protected under *Carpenter v. United States* based on differences in how the data is disclosed. *See supra* notes 233–34 and accompanying text.

sensitive private data. The European Union's General Data Protection Regulation ("GDPR") may represent a viable path for a comprehensive U.S. privacy law.[366] To be sure, the GDPR offers only limited protections for consumer data.[367] It is based largely on principles of control and consent, and it typically places the burden of data protection on users.[368] But its protections may nonetheless be sufficient to eliminate some markets in sensitive consumer data.

The GDPR generally requires users to consent to each particular use of their data, so that data collected for one purpose (like giving accurate weather forecasts) cannot be used for another purpose (like selling data to marketing companies) without express consumer permission.[369] App companies might be able to convince many consumers to consent to the sale of their data by conditioning free or cheap service on such sales, or perhaps by manipulation, deceptive design, or simple consumer fatigue.[370] But an express consent requirement would likely eliminate further downstream sales of consumer data. An entity that purchases data from an app company would be a "controller" of the data under the GDPR, and would assume various responsibilities, including the responsibility to obtain consumer consent for further uses of the data, such as selling it to a law enforcement agency.[371] Users would likely have no reason to give such consent; they have no direct relationship with the data broker, and allowing law enforcement to obtain their data has no benefits and several risks and harms. The adoption of a GDPR-style comprehensive privacy regime is increasingly likely at the federal and/or state levels, due to the benefits of legal standardization and the EU's influence over American companies.[372] Under such a law, today's unregulated markets in sensitive consumer data may be significantly curtailed or largely eliminated.

Other proposed privacy law regimes would focus less on consent and more on directly constraining the collection and harmful use of consumer data.[373] Such approaches would likely curtail markets in sensitive private data and eliminate sales to law enforcement. For example, laws imposing a robust duty of loyalty on companies collecting personal data would prohibit handling data in a manner

366. *See* Hartzog & Richards, *supra* note 251, at 1694–95.

367. *Id.* at 1734.

368. *Id.* at 1734–35.

369. Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1, 4 (EU).

370. *See* Richards & Hartzog, *supra* note 37, at 1478–79; Ari Ezra Waldman, *Privacy's Law of Design*, 9 U.C. IRVINE L. REV. 1239, 1255 (2019).

371. Council Regulation 2016/679, art. 4, 2016 O.J. (L 119) 7 (EU).

372. *See* Hartzog & Richards, *supra* note 251, at 1713.

373. *See* Neil Richards & Woodrow Hartzog, *A Duty of Loyalty for Privacy Law*, 99 WASH. U. L. REV. 961, 997 (2021); Jack M. Balkin, *Information Fiduciaries and the First Amendment*, 49 U.C. DAVIS L. REV. 1183, 1186 (2016).

that conflicts with a user's best interests.[374] Such a standard may prohibit selling user data to third-party advertisers (unless the benefits of the advertising to the user outweigh its privacy harms) and would almost certainly prohibit selling it to data brokers who might then sell it to law enforcement.[375] Again, sales to data brokers or law enforcement entities have little or no benefit to users and carry substantial downsides. Likewise, laws that overtly limit data collection or mandate deletion after use would put an end to secondary markets in consumer data. Companies cannot sell data that they do not collect or retain.[376] Finally, laws that prohibit the deanonymization of consumer data could, if supported by substantial penalties, render useless any location or other data that government entities purchase.[377] Law enforcement tracking of suspects is personalized and individualized, and it depends on deanonymization of digital data, either by contractors working with law enforcement or the officers themselves.[378] There are a variety of potential legal regimes that would regulate markets in private data and eliminate data sales to law enforcement agencies.

3. Regulatory

Finally, federal agencies with regulatory authority over commercial transactions could take a more proactive approach to safeguarding consumer privacy. The Federal Trade Commission ("FTC") is the primary regulator of consumer privacy in the United States, via two types of enforcement.[379] The FTC ensures that companies comply with their own privacy policies, through its authority to police unfair and deceptive trade practices.[380] It also enforces sectoral privacy statutes including the Fair Credit Reporting Act and Children's Online Privacy Protection Act.[381] FTC enforcement is generally limited to egregious cases of deception and has not yet had much impact on app companies selling consumer data

374. *See* Richards & Hartzog, *supra* note 373, at 966.

375. *See id.* at 1019 (discussing the possibility that a duty of loyalty might end targeted advertising in general); Balkin, *supra* note 373, at 1227 (stating that information fiduciaries must not use data "in unexpected ways to the disadvantage of people who use their services or in ways that violate some other important social norm").

376. *See* Hartzog & Richards, *supra* note 251, at 1753.

377. *See id.* at 1754.

378. *See* Burke & Dearen, *supra* note 8; Levinson, *supra* note 105; Tau & Hackman, *supra* note 1.

379. *See* Daniel J. Solove & Woodrow Hartzog, *The FTC and the New Common Law of Privacy*, 114 COLUM. L. REV. 583, 585 (2014).

380. *See id.*; 15 U.S.C. § 45(a)(1); *A Brief Overview of the Federal Trade Commission's Investigative, Law Enforcement, and Rulemaking Authority*, FED. TRADE COMM'N (May 2021), http://www.ftc.gov/about-ftc/mission/enforcement-authority.

381. Solove & Hartzog, *supra* note 379, at 585, 585 n.2.

to data brokers or specialized contractors selling personalized data to law enforcement.[382] But the FTC could adopt a new regulatory regime that adopts substantive limits on data processing rather than mere procedural protections.[383] Indeed, current FTC Chair Lina Khan has raised this possibility in recent public statements.[384]

This more substantive regulation might take any of several forms. The FTC could start enforcing robust Fair Information Practices ("FIPs") similar to those enshrined in the GDPR.[385] Standard FIPs include a requirement that data used for one purpose cannot be used for another without additional consent.[386] As in the GDPR context, this requirement would likely eliminate downstream sales of sensitive consumer data, particularly sales to law enforcement agencies.[387]

The FTC might alternatively use its rulemaking authority under Section 18 of the FTC Act, which empowers it to make rules addressing "unfair or deceptive acts."[388] These rules could specifically identify selling consumer data to law enforcement as an unfair commercial practice subject to FTC enforcement.[389] By law, the FTC would have to establish that selling personal data to law enforcement agencies "causes or is likely to cause substantial injury to consumers which is not reasonably avoidable by consumers themselves and not outweighed by countervailing benefits to consumers or to competition."[390] While sales of protected data to government entities may have law enforcement benefits, they offer few benefits to consumers or competitive consumer-facing markets. Neither are downstream sales of personal data likely to be reasonably avoidable by consumers, who are likely unaware of such sales.[391]

Lastly, the FTC might start to enforce a framework it has already proposed, encouraging companies to adopt "privacy by design."[392] In

382. *See id.* at 656, 674.

383. *See* Lina Khan Remarks, *supra* note 53, at 6.

384. *See id.*

385. *See* Solove & Hartzog, *supra* note 379, at 675. FIPs were originally developed by a United States federal agency in the early 1970s. Hartzog & Richards, *supra* note 251, at 1700. They influenced privacy legislation and private data guidelines throughout the world in subsequent decades, although they have not yet been adopted into federal law in the United States. *Id.* at 1701.

386. Hartzog & Richards, *supra* note 251, at 1700–01.

387. *See* Council Regulation 2016/679, art. 6, 2016 O.J. (L 119) 1, 4 (EU).

388. 15 U.S.C. § 57a(a)(1)(B).

389. *See id.*; 15 U.S.C. § 45(a)(1). The FTC has already sued one data broker selling detailed location data with lax gatekeeping to prevent malicious uses of the data. *See* Complaint for Permanent Injunction and Other Relief at 1, Fed. Trade Comm'n v. Kochava Inc., No. 2:22-cv-377 (D. Idaho Aug. 29, 2022).

390. 15 U.S.C. § 45(n).

391. *See* Richards & Hartzog, *supra* note 37, at 1485, 1497.

392. FED. TRADE COMM'N, PROTECTING CONSUMER PRIVACY IN AN ERA OF RAPID CHANGE: RECOMMENDATIONS FOR BUSINESSES AND POLICYMAKERS 27–28 (Mar.

a 2012 report, the agency called on private companies to promote consumer privacy "throughout their organizations and at every stage of the development of their products and services."[393] Among other principles, this would require companies to adopt limits on their collection and retention of data.[394] Companies would only collect the data they need to accomplish a specific business purpose (like providing weather updates or transportation services) and delete the data once it has fulfilled that purpose.[395] Such a requirement would likely eliminate or substantially curtail secondary markets in previously collected consumer data and would likely preclude additional sales to law enforcement.[396] To date, the FTC's recommendations for privacy by design have had little impact, largely because they were never adopted as mandatory rules or enforcement guidelines.[397] But the FTC could start requiring such practices, characterizing the failure to abide by them as an unfair or deceptive trade practice subject to FTC enforcement via lawsuit.[398]

CONCLUSION

The United States lacks a comprehensive data privacy statute and imposes only minimal legal constraints on consumer data processing.[399] As this Article has detailed, this regulatory vacuum has given rise to commercial markets in sensitive private data.[400] These markets now threaten to erode Fourth Amendment rights in personal data, as law enforcement agencies and police departments across the country have begun to purchase private data for law enforcement and other purposes.[401] This Article has comprehensively analyzed the legality of these purchases. Ultimately, it demonstrates

---

2012) [hereinafter FTC Consumer Privacy Report], http://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf.

393. *Id.* at 22.

394. *Id.* at 26; *see* Waldman, *supra* note 370, at 1244; WOODROW HARTZOG, PRIVACY'S BLUEPRINT: THE BATTLE TO CONTROL THE DESIGN OF NEW TECHNOLOGIES 22–26 (2018).

395. FTC Consumer Privacy Report, *supra* note 392, at 26–28.

396. To be sure, the FTC report suggested that companies might be able to justify data practices that go beyond those uses that will be apparent to consumers with sufficient consumer consent. *Id.* at 48. But even this appears to contemplate consumer consent for each subsequent use of data, which would likely preclude third-party sales by data brokers. *See supra* note 372 and accompanying text.

397. *See* FTC Consumer Privacy Report, *supra* note 392, at 22.

398. *See* 15 U.S.C. § 57a(a)(1)(B).

399. *See, e.g.*, Hartzog & Richards, *supra* note 251, at 1690, 1697.

400. *See supra* Subparts I.C, IV.A.

401. *See supra* Subpart I.C.

that warrantless government purchases of sensitive personal data violate the Fourth Amendment.

The revealing information purchased by government entities is not commercially available to the public, is not in general public use, and does not lose its constitutional protections just because the government pays money to another party to obtain it.[402] It accordingly remains private for Fourth Amendment purposes. Moreover, longstanding anti-evasion principles embedded in constitutional law prevent the government from circumventing the Supreme Court rulings establishing Fourth Amendment rights in private data.[403]

Nor do the permissions that consumers give to apps and service providers strip their digital data of all constitutional protection. These narrow permissions are inadequate to waive users' Fourth Amendment rights against government searches.[404] And much of the data at issue is disclosed to apps automatically, without consumer input, in contexts where users have little choice but to comply.[405] This sensitive, often intimate data retains its Fourth Amendment protections notwithstanding its limited disclosure to other parties.

In recent years, many government entities have argued that purchasing private data offers a way around constitutional restrictions, allowing the government to obtain Fourth Amendment-protected data without complying with the Amendment's requirements.[406] This Article has sought to bring this attempt at constitutional evasion to light, and to propose ways that courts and other legal actors can prevent it, before it undermines the Fourth Amendment. The time has come for judges, lawmakers, and regulators to recognize the unique threat to privacy posed by government agents buying our personal data.

402. *See supra* Part II.
403. *See supra* Subpart II.C.
404. *See supra* Subpart III.A.
405. *See supra* Subpart III.B.
406. *See supra* notes 15, 233–34 and accompanying text.