The Clocks Are Striking Thirteen: Congress, Not Courts, Must Save Us from Government Surveillance via Data Brokers

Andrew Wade[*]

Can the government buy its way around the Fourth Amendment's warrant requirement? As the panic over data-sharing after Dobbs *illustrates, the answer is an urgent yes. Transactions between the government and data brokers—businesses that acquire, aggregate, and sell massive amounts of data on individuals' digital activities—fall outside the Stored Communications Act's hopelessly out-of-date guardrails and through a Fourth Amendment "loophole." Though the Supreme Court's 2018* Carpenter *decision provides a useful framework for evaluating data's Fourth Amendment protection, it will not save us from data brokers. The "tick–tick–tock" cycle of Fourth Amendment precedent and privacy legislation is off. As Orwell would say, the clocks are "striking thirteen." It is past time for Congress to pass new privacy legislation.*

But what should that legislation look like? History, as usual, offers clues. In this Note, I argue that to rebalance competing interests in light of paradigm technological change, Congress must learn from past mistakes in drafting the Stored Communications Act. I analyze three potential legislative solutions—the Fourth Amendment Is Not for Sale Act; the My Body, My Data Act; and California's "Delete Act"—and propose my own, which combines the strengths of each and provides flexibility for future technological developments. That way, when the Fourth Amendment clock strikes again, we will be ready.

* Research Editor, Volume 102, *Texas Law Review*; J.D. Candidate, Class of 2024, The University of Texas School of Law. Special thanks to Professor Chinmayi Sharma for introducing me to this fascinating intersection between dusty constitutional doctrines and cutting-edge technology. A sincere thanks also to my wife, Natalie, for her unwavering patience and support; to my brother, Jack Wade, for serving as a sounding board and much-needed prosecutorial foil; to our Chief Notes Editor Kelsey Anderson and Notes Editor Benton McDonald for their tireless efforts to push this Note to the next level; and to our hardworking *Texas Law Review* New Members for their thorough and thoughtful edits.

Introduction

George Orwell introduced his *1984* dystopia with an unsettling image: "It was a bright cold day in April, and the clocks were striking thirteen."[1] On May 2, 2022, a leaked draft of the Supreme Court's *Dobbs v. Jackson Women's Health Organization*[2] decision, which revoked the constitutional right to abortion,[3] produced such a resounding clamor over menstrual-tracking apps and data sharing that it at once became clear that the clocks were striking thirteen on government surveillance via data brokers:

1. George Orwell, 1984, at 3 (Alma Classics ed., 2021).

2. 142 S. Ct. 2228 (2022). For more information on the leak, see generally Josh Gerstein & Alexander Ward, *Supreme Court Has Voted to Overturn Abortion Rights, Draft Opinion Shows*, POLITICO (May 3, 2022, 2:14 PM), https://www.politico.com/news/2022/05/02/supreme-court-abortion-draft-opinion-00029473 [https://perma.cc/Y4K2-WRW6]; *see also* Jesus Jiménez, *After the Supreme Court's Leaked Draft, What Happens Next?*, N.Y. TIMES (May 3, 2022), https://www.nytimes.com/2022/05/03/us/roe-wade-supreme-court-what-next.html?smid=url-share [https://perma.cc/JU96-PSQP] (describing the leaked *Dobbs* opinion's potential impact).

3. *Dobbs*, 142 S. Ct. at 2284.

companies that, largely without Americans' knowledge or consent, collect billions of data elements about them, aggregate them into detailed consumer profiles, and sell these profiles to third parties.[4]

Well before *Dobbs* leaked, the Secret Service, IRS, U.S. military, DEA, ICE, CBP, FBI, and governmental entities at the state and local levels had all purchased data from brokers without obtaining Fourth Amendment search warrants.[5] Lawmakers had already begun investigating these entities for

4. FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY i, iv–v (May 2014), https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf [https://perma.cc/S4RZ-PCLQ]. Data brokers collect personal information such as names, addresses, phone numbers, email addresses, Social Security and driver's license numbers, birth dates, age, gender, ethnicity, country of origin, languages spoken, height, weight, health information, marital status, household size (including information about cohabitating children, elderly family members, and pets), education level, occupation, estimated income, religion, voting registration, political party identification, recent purchase activity, consumer preferences, and even real-time location data. *Id.* at app. B 3–6; *Data Brokers*, ELEC. PRIV. INFO. CTR., https://epic.org/issues/consumer-privacy/data-brokers [https://perma.cc/28G5-3AF2].

5. *E.g.*, Adi Robertson, *Secret Service Bought Access to Cellphone Location Data*, VERGE (Aug. 17, 2020, 3:47 PM), https://www.theverge.com/2020/8/17/21371886/secret-service-usss-locate-x-babel-street-foia-contract-report [https://perma.cc/F5N5-XQBY]; Joseph Cox, *The IRS Is Being Investigated for Using Location Data Without a Warrant*, VICE: MOTHERBOARD (Oct. 6, 2020, 4:47 PM), https://www.vice.com/en/article/qj479d/irs-investigation-location-data-no-warrant-venntel [https://perma.cc/C23X-TNTT]; Byron Tau, *IRS Used Cellphone Location Data to Try to Find Suspects*, WALL ST. J. (June 19, 2020, 1:46 PM), https://www.wsj.com/articles/irs-used-cellphone-location-data-to-try-to-find-suspects-11592587815 [https://perma.cc/9ZYY-A5A7]; Joseph Cox, *How the U.S. Military Buys Location Data from Ordinary Apps*, VICE: MOTHERBOARD (Nov. 16, 2020, 3:35 PM) [hereinafter Cox, *U.S. Military Data*], https://www.vice.com/en/article/jgqm5x/us-military-location-data-xmode-locate-x [https://perma.cc/2GNS-XVQM]; Charlie Savage, *Intelligence Analysts Use U.S. Smartphone Location Data Without Warrants, Memo Says*, N.Y. TIMES (Jan. 25, 2021), https://www.nytimes.com/2021/01/22/us/politics/dia-surveillance-data.html [https://perma.cc/TMH3-FA8U]; Joseph Cox, *The DEA Abruptly Cut Off Its App Location Data Contract*, VICE: MOTHERBOARD (Dec. 7, 2020, 8:00 AM) [hereinafter Cox, *DEA Contract*], https://www.vice.com/en/article/z3v3yy/dea-venntel-location-data [https://perma.cc/2TE2-U3HY]; Joseph Cox, *How an ICE Contractor Tracks Phones Around the World*, VICE: MOTHERBOARD (Dec. 3, 2020, 5:35 AM) [hereinafter Cox, *ICE Tracking*], https://www.vice.com/en/article/epdpdm/ice-dhs-fbi-location-data-venntel-apps [https://perma.cc/UV2F-DT4S]; Byron Tau & Michelle Hackman, *Federal Agencies Use Cellphone Location Data for Immigration Enforcement*, WALL ST. J. (Feb. 7, 2020, 7:30 AM), https://www.wsj.com/articles/federal-agencies-use-cellphone-location-data-for-immigration-enforcement-11581078600?mod=article_inline [https://perma.cc/GN83-P5ZQ]; Joseph Cox, *Here Is the FBI's Contract to Buy Mass Internet Data*, VICE: MOTHERBOARD (Mar. 27, 2023, 8:00 AM) [hereinafter Cox, *FBI Netflow Data*], https://www.vice.com/en/article/dy3z9a/fbi-bought-netflow-data-team-cymru-contract [https://perma.cc/S7CD-LULH]; Joseph Cox, *Florida Prison System Bought Location Data from Apps*, VICE: MOTHERBOARD (Mar. 10, 2021, 2:00 PM) [hereinafter Cox, *Florida Prisons*], https://www.vice.com/en/article/3an9jy/florida-prison-locate-x-location-data-department-of-corrections [https://perma.cc/4845-HCJ9]; Garance Burke & Jason Dearen, *Tech Tool Offers Police 'Mass Surveillance on a Budget,'* ASSOCIATED PRESS (Sept. 2, 2022, 9:28 PM), https://apnews.com/article/technology-police-government-surveillance-d395409ef5a8c6c3f6cdab5b1d0e27ef [https://perma.cc/Q68R-PUGX].

"buy[ing] [their] way around the Fourth Amendment."[6] And in 2021, Senators Wyden, Paul, Daines, and Lee proposed the Fourth Amendment Is Not for Sale Act to close gaping loopholes in the Electronic Communication Privacy Act of 1986 that enable the government to "us[e] its credit card to erase Americans' Constitutional rights."[7] Curiously, governmental entities had bought data from these "shady middlemen"[8] despite the Supreme Court's 2018 decision in *Carpenter v. United States*,[9] which held that a warrant was required to obtain a week's worth of location data from wireless carriers.[10] By May 2022, governmental entities could *buy* the same data for a little over $160.[11] And they claimed it was perfectly legal.[12]

Within days of the *Dobbs* leak, data brokers became the subjects of intense public scrutiny.[13] Vice News's Motherboard reported that the data

6. Letter from Elizabeth Warren, Carolyn B. Maloney, Ron Wyden & Mark DeSaulnier, U.S. Sens. & Members of Congress, to Anindya Datta, CEO and Chairman of Mobilewalla (Aug. 3, 2020), https://www.warren.senate.gov/imo/media/doc/2020.08.03%20Letter%20to%20data%20broker%20Mobilewalla.pdf [https://perma.cc/57PB-EQJX]; *see id.* (requesting information regarding the "surveillance" of Americans participating in protests).

7. Ron Wyden, U.S. Sen., Wyden Remarks on Secret Law and the Fourth Amendment Is Not for Sale Act for the Cato Institute 1–2, 5 (Dec. 14, 2021) [hereinafter Wyden Remarks], https://www.wyden.senate.gov/imo/media/doc/Wyden%20Cato%20Institute%20Remarks%20on%20Secret%20Law%20and%20the%20Fourth%20Amendment%20is%20Not%20For%20Sale%20Act.pdf [https://perma.cc/7BFE-T5W9]. Senators Wyden, Paul, and others reintroduced the Fourth Amendment Is Not for Sale Act in July 2023. Press Release, Ron Wyden, U.S. Sen., Wyden, Paul and Bipartisan Senators Reintroduce the Fourth Amendment Is Not for Sale Act (July 27, 2023) [hereinafter Press Release, Bipartisan Senators Reintroduce the Fourth Amendment Is Not for Sale Act], https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-senators-reintroduce-the-fourth-amendment-is-not-for-sale-act [https://perma.cc/5P7X-FJN2]; Fourth Amendment Is Not for Sale Act, S. 2576, 118th Cong. (2023), https://www.congress.gov/118/bills/s2576/BILLS-118s2576is.pdf [https://perma.cc/K4NB-TYZY]. The text of the 2023 bill is identical to that of the 2021 bill. *Compare id.*, *with* Fourth Amendment Is Not for Sale Act, S. 1265, 117th Cong. (2021), https://www.congress.gov/117/bills/s1265/BILLS-117s1265is.pdf [https://perma.cc/2WC7-3JBB].

8. Wyden Remarks, *supra* note 7, at 2, 4–5.

9. 138 S. Ct. 2206 (2018).

10. *Id.* at 2217 & n.3, 2219, 2221.

11. Joseph Cox, *Data Broker Is Selling Location Data of People Who Visit Abortion Clinics*, VICE: MOTHERBOARD (May 3, 2022, 11:46 AM) [hereinafter Cox, *SafeGraph*], https://www.vice.com/en/article/m7vzjb/location-data-abortion-clinics-safegraph-planned-parenthood [https://perma.cc/J35N-CLRR].

12. *See, e.g.*, Letter from J. Russell George, Inspector Gen. for Tax Admin., Dep't of Treasury, to Ron Wyden and Elizabeth Warren. U.S. Sens. (Feb. 18, 2021), https://s3.documentcloud.org/documents/20490079/response.pdf [https://perma.cc/G4FV-D5UN] (distinguishing involuntarily shared cell-site location information in *Carpenter* from "opt-in app data" available on a data broker's platform).

13. *See* Cox, *SafeGraph*, *supra* note 11 (describing how easily and inexpensively one could purchase abortion clinic-related location data for vigilantism and surveillance in an article published shortly after the leak); Joseph Cox, *Location Data Firm Provides Heat Maps of Where Abortion Clinic Visitors Live*, VICE: MOTHERBOARD (May 5, 2022, 12:24 PM) [hereinafter Cox, *Placer.ai*],

broker SafeGraph was offering its users a bird's-eye view of every tracked device traveling in and out of any of 600 Planned Parenthood locations across the United States.[14] Though SafeGraph claimed its data was anonymized, a motivated individual could analyze attributes, such as device operating system, to easily unmask individuals, especially when some datasets contained as few as four or five devices.[15]

That same week, Motherboard revealed that another data broker, Placer.ai, had used location data to generate "heat maps" showing the approximate areas where Planned Parenthood clinic visitors lived, their likely demographic information, and places they had visited since.[16] Previously, pro-life activists had used broker data to send targeted ads to clinic visitors' phones.[17] Now, they could use it to track, sue, or prosecute clinics providing out-of-state abortions.[18] All it would take is a few minutes to make a free account.[19]

With *Roe*'s future uncertain, many women deleted menstrual-tracking apps from their phones, fearing the apps might share their reproductive health data with third parties, including data brokers and eventually law enforcement.[20] Google announced it would automatically delete medical clinic visits from users' location history.[21] The Federal Trade Commission (FTC) asserted it would "vigorously" enforce laws protecting Americans' sensitive data.[22] Fourteen senators and the House Committee on Oversight

---

https://www.vice.com/en/article/g5qaq3/location-data-firm-heat-maps-planned-parenthood-abortion-clinics-placer-ai [https://perma.cc/BP3E-FVP6] (explaining how one platform's heat maps of patients' approximate residences could reveal which clinics performed out-of-state abortions).

14. Cox, *SafeGraph*, *supra* note 11.

15. *Id.*; *see* Natasha Lomas, *Researchers Spotlight the Lie of 'Anonymous' Data*, TECHCRUNCH (July 24, 2019, 10:30 AM), https://techcrunch.com/2019/07/24/researchers-spotlight-the-lie-of-anonymous-data [https://perma.cc/T4AZ-JB8F] (describing how researchers successfully re-identified 99.98% of individuals in anonymized datasets using only fifteen demographic attributes).

16. Cox, *Placer.ai*, *supra* note 13.

17. *Id.*; *cf.* Bob Salsberg, *Agreement Bars Ad Firm from Targeting Women Entering Clinics*, ASSOCIATED PRESS (Apr. 4, 2017, 4:11 PM), https://apnews.com/33f18b834c104df9b2901ef1bf38ae08/Agreement-bars-ad-firm-from-targeting-women-entering-clinics [https://perma.cc/G853-H5S8] (explaining how Massachusetts ended the practice with one advertising firm via settlement).

18. Cox, *Placer.ai*, *supra* note 13.

19. *Id.*

20. Tatum Hunter & Heather Kelly, *With* Roe *Overturned, Period-Tracking Apps Raise New Worries*, WASH. POST (June 24, 2022, 2:30 PM), https://www.washingtonpost.com/technology/2022/05/07/period-tracking-privacy/?itid=ap_tatumhunter [https://perma.cc/B88F-PSQK].

21. Jen Fitzpatrick, *Protecting People's Privacy on Health Topics*, GOOGLE: THE KEYWORD (July 1, 2022), https://blog.google/technology/safety-security/protecting-peoples-privacy-on-health-topics [https://perma.cc/K37Z-AVQ4].

22. Kristin Cohen, *Location, Health, and Other Sensitive Information: FTC Committed to Fully Enforcing the Law Against Illegal Use and Sharing of Highly Sensitive Data*, FED. TRADE COMM.: BUS. BLOG (July 11, 2022), https://www.ftc.gov/business-guidance/blog/2022/07/location-health-

and Reform sent letters to SafeGraph, Placer.ai, and other data brokers seeking information about their collection and sale of location and reproductive health data, which could "facilitat[e] intrusive government surveillance."[23] House Representative Sara Jacobs proposed the My Body, My Data Act to preemptively protect personal reproductive health data from disclosure and government misuse.[24] Once-hypothetical fears that the government would wield its citizens' personal data against them suddenly became more salient.[25] "This isn't the stuff of dystopian fiction," the FTC cautioned.[26] "It's a question consumers are asking right now."[27]

Whatever one thinks about *Dobbs*, the government's unrestrained ability to buy sensitive data without a warrant thwarts the Fourth Amendment's intended purposes, erodes our rights, and raises serious questions about digital searches that neither courts nor Congress have fully answered. This Note evaluates the modern history of Fourth Amendment doctrine, explains why *Carpenter* and the courts cannot save us from data brokers, and argues that Congress must intervene by passing new privacy legislation. After reviewing the strengths and weaknesses of two proposed

---

and-other-sensitive-information-ftc-committed-fully-enforcing-law-against-illegal [https://perma.cc/M3JE-MJ6F].

23. Press Release, House Comm. on Oversight & Acct., Maloney, Krishnamoorthi, and Jacobs Launch Probe of Reproductive Health Data Privacy (July 8, 2022), https://oversightdemocrats.house.gov/news/press-releases/maloney-krishnamoorthi-and-jacobs-launch-probe-of-reproductive-health-data [https://perma.cc/NKA2-MPW6]; Letter from Elizabeth Warren, Tammy Baldwin, Patty Murray, Tina Smith, Bernard Sanders, Edward J. Markey, Richard Blumenthal, Cory A. Booker, Amy Klobuchar, Christopher S. Murphy, Ron Wyden, Tammy Duckworth, Alex Padilla, and Ben Ray Lujan, U.S. Sens., to Auren Hoffman, CEO of SafeGraph, Inc. (May 17, 2022), https://www.warren.senate.gov/imo/media/doc/2022.05.17%20Letters%20to%20Safegraph%20and%20Placer.ai%20re%20Abortion%20Clinic%20Data.pdf [https://perma.cc/U649-U6DH]; Letter from Elizabeth Warren, Tammy Baldwin, Patty Murray, Tina Smith, Bernard Sanders, Edward J. Markey, Richard Blumenthal, Cory A. Booker, Amy Klobuchar, Christopher S. Murphy, Ron Wyden, Tammy Duckworth, Alex Padilla, and Ben Ray Lujan, U.S. Sens., to Noam Ben-Zvi, CEO of Placer.ai (May 17, 2022), https://www.warren.senate.gov/imo/media/doc/2022.05.17%20Letters%20to%20Safegraph%20and%20Placer.ai%20re%20Abortion%20Clinic%20Data.pdf [https://perma.cc/U649-U6DH].

24. Press Release, Congresswoman Sara Jacobs, Congresswoman Jacobs Announces My Body, My Data Act to Protect Reproductive Health Data (June 2, 2022), https://sarajacobs.house.gov/news/documentsingle.aspx?DocumentID=542 [https://perma.cc/2SQJ-YHJR]. Representative Jacobs introduced a revised version of the bill in May 2023. Press Release, Congresswoman Sara Jacobs, Rep. Sara Jacobs Leads Reintroduction of My Body, My Data Act to Protect Reproductive and Sexual Health Data (May 17, 2023), https://sarajacobs.house.gov/news/documentsingle.aspx?DocumentID=786 [https://perma.cc/39PP-ESMD]; My Body, My Data Act of 2023, H.R. 3420, 118th Cong. (2023).

25. *See* Jay Edelson, *Post*-Dobbs, *Your Private Data Will Be Used Against You*, BLOOMBERG L. (Sept. 22, 2022, 3:00 AM), https://news.bloomberglaw.com/us-law-week/post-dobbs-your-private-data-will-be-used-against-you [https://perma.cc/KR9U-T2F3] ("Location data will show if you visited an abortion provider. Search history will record that you Googled an abortifacient. Period-tracking apps can reveal that you missed your last period.").

26. Cohen, *supra* note 22.

27. *Id.*

federal privacy laws (the Fourth Amendment Is Not for Sale Act and the My Body, My Data Act) and California's recently enacted "Delete Act," I propose my own solution that incorporates lessons from the past and safeguards for the future.

I. Why the Government Might Want to Purchase Broker Data

The government might choose to buy broker data for numerous reasons. First, broker data provides the government with cheap mass surveillance, helping it identify where criminal activity is generally occurring. U.S. Customs and Border Protection, for example, has purchased location data from brokers to detect the movement of undocumented immigrants by pointing to cell phone activity in suspicious locations, such as the deserts along the U.S.–Mexico border.[28] At the state level, the Florida Department of Corrections has also bought device location data,[29] presumably to find cell phones that inmates illegally possessed, that it could use to track *all* cell phones entering and exiting its prisons and where those devices traveled next.

Mass digital surveillance of this sort produces the same societal costs that mass physical surveillance always has, what Professor Mary Fan in this issue calls *collateral impact* and *collateral harm*: innocent people will be implicated—and possibly harmed—simply for living in a heavily policed neighborhood or otherwise being in the wrong place at the wrong time.[30] But digital surveillance is more comprehensive than physical surveillance, and unlike physical surveillance, it requires neither a big budget nor a large number of boots on the ground.[31] So, unless legal barriers are put in place, collateral impact and harm will rise as law enforcement increasingly substitutes (or at least supplements) mass physical surveillance with mass digital surveillance.

Second, broker data may help the government identify specific devices and people involved in criminal activity. The FBI has purchased "netflow" data, which allows it to track traffic through VPNs and locate hacker infrastructure, and which may also reveal users' browsing history.[32] The Secret Service has reportedly purchased location data to seize illegal credit card skimmers installed in gas pumps.[33] As for identifying people, the

28. Tau & Hackman, *supra* note 5.

29. Cox, *Florida Prisons*, *supra* note 5.

30. Mary D. Fan, *Big Data Searches and the Future of Criminal Procedure*, 102 TEXAS L. REV. 877, 886 (2024); Matthew Guariglia, *What Is Fog Data Science? Why Is the Surveillance Company So Dangerous?*, ELEC. FRONTIER FOUND. (Aug. 31, 2022), https://www.eff.org/deeplinks/2022/06/what-fog-data-science-why-surveillance-company-so-dangerous [https://perma.cc/F4UQ-Y3R4].

31. *See* Burke & Dearen, *supra* note 5 (quoting data broker's claim that it "fill[s] a gap for underfunded and understaffed departments").

32. Cox, *FBI Netflow Data*, *supra* note 5.

33. Robertson, *supra* note 5.

Internal Revenue Service tried (unsuccessfully, it claims) to pinpoint tax offenders by cross-referencing purchased location data with its knowledge about where suspicious transactions took place.[34] The Drug Enforcement Administration made similar attempts but canceled its contract without explanation.[35] Other governmental entities, however, may have better luck. Immigration and Customs Enforcement has successfully used purchased location data to identify immigrants who were later arrested.[36] Local law enforcement has bought location data to find murderers and human traffickers by searching for devices present at crime scenes.[37] But police could buy other data to catch more mundane offenders, like speeding drivers.[38] Using geofence warrants,[39] federal law enforcement has obtained Google location data to look for arsonists at Black Lives Matter protests[40] and prosecute armed insurrectionists at the U.S. Capitol on January 6, 2021.[41] But without probable cause standing in its way, the government could just as

34. Tau, *supra* note 5.

35. Cox, *DEA Contract*, *supra* note 5.

36. Cox, *ICE Tracking*, *supra* note 5.

37. Burke & Dearen, *supra* note 5.

38. *C.f.* Kashmir Hill, *Automakers Are Sharing Consumers' Driving Behavior with Insurance Companies*, N.Y. TIMES (Mar. 11, 2024), https://www.nytimes.com/2024/03/11/technology/carmakers-driver-tracking-insurance.html [https://perma.cc/5UUG-8PBY] (describing how one data broker obtains encyclopedic information about individuals' driving behavior, including speeding, from car manufacturers and sells it to insurance companies—sometimes without those individuals' knowledge or consent).

39. Unlike data broker purchases, geofence warrants require probable cause and particularization. *E.g.*, United States v. Rhine, No. 21-0687, 2023 WL 372044, at *20 (D.D.C. Jan. 24, 2023). Though geofence warrants are a seemingly legitimate alternative to warrantless broker data purchases, they may take days or weeks to get. Burke & Dearen, *supra* note 5. Courts and scholars are split on whether geofence warrants are constitutional. *Compare* Haley Amster & Brett Diehl, Note, *Against Geofences*, 74 STAN. L. REV. 385, 429–33 (2022) (arguing that geofence warrants flunk the Fourth Amendment's probable cause and particularity requirements because they target broad locations, not a specific user or set of users), *with* Fan, *supra* note 30, at 932–34 (countering that "imagining a possible worst-case abuse of an investigative strategy is usually not a basis for a constitutional straightjacket prohibiting the practice altogether" and proposing principles for "digital probable cause"). Some have argued that the way courts approach geofence warrants may explain how they eventually analyze government purchases of broker data under the Fourth Amendment. *E.g.*, Dori H. Rahbar, Note, *Laundering Data: How the Government's Purchase of Commercial Location Data Violates* Carpenter *and Evades the Fourth Amendment*, 122 COLUM. L. REV. 713, 733 (2022). But we cannot afford to wait for courts to parse through these complicated questions; to protect our fundamental rights, Congress must intervene by passing privacy legislation now. *See infra* Part IV.

40. Zack Whittaker, *Minneapolis Police Tapped Google to Identify George Floyd Protesters*, TECHCRUNCH (Feb. 6, 2021, 4:00 PM), https://tcrn.ch/39VRPA1 [https://perma.cc/ZE8T-NSN6]; Corin Faife, *FBI Used Geofence Warrant in Seattle After BLM Protest Attack, New Documents Show*, VERGE (Feb. 5, 2022, 2:00 PM), https://www.theverge.com/2022/2/5/22918487/fbi-geofence-seattle-blm-protest-police-guild-attack [https://perma.cc/SA2T-2SLV].

41. *E.g.*, *Rhine*, 2023 WL 372044, at *19–20, *27.

easily use broker data to target peaceful protestors for expressing their views.[42]

Third, governmental entities might use broker data for smarter transportation, public health, military, and marketing campaigns. For example, the Illinois Department of Transportation purchased SafeGraph location data so its consultants could mine it for traffic pattern insights.[43] In 2020, Washington, D.C.'s local government accepted a data broker's offer to freely use six months of anonymized, GPS-level location data for COVID-19 tracking and response efforts.[44] Similarly, the CDC used SafeGraph's aggregated location data to monitor compliance with COVID-19 curfews and social distancing restrictions, but also saw its potential for use in research about "travel to parks and green spaces, physical activity and mode of travel, and population migration before, during, and after natural disasters."[45] The United States Special Operations Command, a branch of the military tasked with counterterrorism, counterinsurgency, and special reconnaissance, may have used purchased location data to target drone strikes.[46] And the Georgia National Guard has, through a digital marketing agency, used broker data for recruiting by "geofencing" Atlanta-area high schools to serve targeted ads to students.[47] But nothing stops the state national guard's recruiters from purchasing the same data for direct, internal use.

Reasonable minds may differ on the extent to which government *should* have access to broker data. After all, private actors already do, and law enforcement might legitimately need access to keep pace with

42. Lawmakers have also expressed this concern. *Warren, Maloney, Wyden, DeSaulnier Probe Data Broker's Collection of Data on Black Lives Matter Demonstrators*, ELIZABETH WARREN (Aug. 4, 2020), https://www.warren.senate.gov/oversight/letters/warren-maloney-wyden-desaulnier-probe-data-brokers-collection-of-data-on-black-lives-matter-demonstrators [https://perma.cc/JJB6-258A].

43. Bennett Cyphers & Jason Kelley, *Illinois Bought Invasive Phone Location Data from Banned Broker Safegraph*, ELEC. FRONTIER FOUND. (Aug. 19, 2021), https://www.eff.org/deeplinks/2021/08/illinois-bought-invasive-phone-location-data-banned-broker-safegraph [https://perma.cc/7Y36-3XCB].

44. Bennett Cyphers, *Data Broker Veraset Gave Bulk Device-Level GPS Data to DC Government*, ELEC. FRONTIER FOUND. (Nov. 10, 2021), https://www.eff.org/deeplinks/2021/11/data-broker-veraset-gave-bulk-device-level-gps-data-dc-government [https://perma.cc/7DQC-YYN9]. After the trial period ended, officials retained that data alongside their own until the end of 2021, *id.*, and may have used it for other purposes.

45. Joseph Cox, *CDC Tracked Millions of Phones to See if Americans Followed COVID Lockdown Orders*, VICE: MOTHERBOARD (May 3, 2022, 8:00 AM), https://www.vice.com/en/article/m7vymn/cdc-tracked-phones-location-data-curfews [https://perma.cc/HC6F-MEYN].

46. Cox, *U.S. Military Data*, *supra* note 5.

47. Doug Reardon, *National Guard Using "Geofencing" Around Area Schools to Recruit New Members*, ATLANTA NEWS FIRST (Apr. 25, 2023, 10:02 PM), https://www.atlantanewsfirst.com/2023/04/25/national-guard-using-geofencing-around-area-schools-recruit-new-members [https://perma.cc/7EQ8-2NLC].

technologically sophisticated criminals.[48] Even if the Fourth Amendment presents (or should present) a barrier to that access, the requirements of probable cause and particularization might need "updating" to evolve with technological realities.[49] But We the People have had no opportunity to consider these questions and strike an appropriate balance. The government has taken the law into its own hands, violating the spirit, if not the letter, of our Constitution.

II. Letting the Government Buy Broker Data without a Warrant Circumvents the Fourth Amendment and Erodes Our Rights to Privacy and Freedom from Arbitrary Power

The Fourth Amendment protects individuals' right "to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures" by the government.[50] It was the Framers' "response to the reviled 'general warrants' and 'writs of assistance' of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity."[51] The Fourth Amendment "secure[s] 'the privacies of life' against 'arbitrary power'" and "place[s] obstacles in the way of a too permeating police surveillance."[52] To conduct a reasonable search under the Fourth Amendment, government officials must ordinarily secure a warrant[53] supported by "probable cause"[54]: when there is a fair probability that evidence of a crime will be found in the place to be searched.[55]

---

48. *Cf.* James B. Comey, *Going Dark: Are Technology, Privacy, and Public Safety on a Collision Course?*, FBI (Oct. 16, 2014), https://www.fbi.gov/news/speeches/going-dark-are-technology-privacy-and-public-safety-on-a-collision-course [https://perma.cc/JR7X-G63T] (arguing that, even with lawful authority to conduct surveillance, law enforcement needs greater access to digital evidence to keep Americans safe from technologically sophisticated criminals); Alistair Simmons, *The Justice Department's Agreement with a Data Broker That Facilitated Elder Fraud*, LAWFARE (Nov. 7, 2022, 8:16 AM) (describing how scammers purchased data brokers' "suckers lists" to target the elderly and other vulnerable people), https://www.lawfaremedia.org/article/justice-departments-agreement-data-broker-facilitated-elder-fraud [https://perma.cc/692R-4GSG]; *see* Reardon, *supra* note 47 (noting that geofence marketing is "no different than what civilian organizations use in their marketing").

49. *See* Fan, *supra* note 30, at 886–87 (proposing new conceptual frameworks for probable cause and particularization for geofence and keyword warrants).

50. U.S. CONST. amend. IV.

51. Riley v. California, 573 U.S. 373, 403 (2014).

52. Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018) (first quoting Boyd v. United States, 116 U.S. 616, 630 (1886), and then quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).

53. Kentucky v. King, 563 U.S. 452, 459 (2011); *see also* Katz v. United States, 389 U.S. 347, 357 (1967) (noting that "[s]earches conducted without warrants have been held unlawful" regardless of probable cause and "are *per se* unreasonable under the Fourth Amendment").

54. U.S. CONST. amend. IV.

55. Illinois v. Gates, 462 U.S. 213, 238 (1983).

When the government buys broker data without probable cause, it flouts our supermajority grant,[56] surreptitiously subjects blameless citizens to "near perfect surveillance,"[57] and recklessly exposes us to risks of stalking, harassment, blackmail, public shaming,[58] and arbitrary persecution for our "familial, political, professional, religious, and sexual associations."[59] Without suitable privacy laws, the Fourth Amendment is the last bulwark standing in the way. And in recent decades, the Supreme Court has largely failed to wield it—despite repeated reports of government abuse.[60]

We cannot afford to shrug off and normalize this infringement. We must enforce the rules *now*.

III. The Modern Development of Fourth Amendment Doctrine and Privacy Law Has Followed a Tick–Tick–*Tock* Cycle

Since at least the 1920s, Fourth Amendment doctrine and privacy law have followed a predictable tick–tick–*tock* cycle. First, some revolutionary technology emerges—the telephone, the wiretap, the pen register, and so on. Law enforcement eagerly exploits this new technology, but in its haste to investigate fails to obtain a warrant. *Tick.* The Supreme Court nods to the technology's growing importance to society, then articulates a broad theory as to why the Fourth Amendment clearly did or did not protect the defendant's privacy. *Tick*. Congress rushes in to clarify the standard. It passes new legislation authorizing the government to use the technology for investigation, but only under carefully prescribed conditions. *Tock*. Repeat.

Professor Orin Kerr would describe the two ticks as "equilibrium adjustment": when technological or social change destabilizes the traditional balance between police power and privacy, courts tighten or loosen Fourth Amendment doctrine "as a correction mechanism" to restore the status quo.[61] This status quo dates to the Founding and is constantly jostled by new technologies, which "enable both cops *and* robbers to accomplish tasks they couldn't before, or else to do old tasks more easily or cheaply."[62] The telephone, for example, gave co-conspirators a new, inconspicuous way to

56. *See* U.S. CONST. art. V (announcing that constitutional amendments must be "ratified by the Legislatures of three fourths of the several States, or by Conventions in three fourths thereof").

57. *See Carpenter*, 138 S. Ct. at 2218 (recognizing that most people today keep their cell phones within five feet everywhere they go, including private places where entirely innocent conduct occurs).

58. OFF. OF THE DIR. OF NAT'L INTEL., PANEL ON COMMERCIALLY AVAILABLE INFORMATION 12 (2022), https://www.dni.gov/files/ODNI/documents/assessments/ODNI-Declassified-Report-on-CAI-January2022.pdf [https://perma.cc/A2W5-Q9NP].

59. United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring).

60. *See supra* note 5 and accompanying text.

61. *E.g.*, Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV. 478, 482, 487 (2011).

62. *Id.* at 483–84, 486 (emphasis added).

communicate—and at the same time gave police a new, unobtrusive way to eavesdrop.[63] Social and political change, too, may disrupt the status quo by begetting new crimes, new ways to commit old crimes, and new investigation methods.[64] But whenever the police power–privacy scale becomes so tipped that "judges . . . fear dystopia," they try—sometimes unsuccessfully—to restore traditional balance.[65]

Kerr's equilibrium-adjustment theory enjoys substantial historical support and intuitive explanatory power.[66] "Almost everyone finds something to like" about it,[67] and I am no exception. But I believe Kerr misinterprets the relationship between judicial equilibrium adjustment and legislative action—between the ticks and the tock of the Fourth Amendment clock. Kerr thinks that when a court intervenes too early in a new technology's life cycle, it cannot accurately gauge the technology's effects, risks misjudging how much equilibrium adjustment is needed, and could delay a final, satisfactory resolution of Fourth Amendment issues.[68] He points to *Olmstead v. United States*[69] as an example: if the Supreme Court had only waited until the telephone was more mature, it would not have taken thirty-nine years to reach the "correct result" in *Katz v. United States*.[70] Judicial delay, according to Kerr, is wise because it invites Congress to craft better solutions in the meantime, whereas "even tentative judicial rulings are likely to keep Congress away."[71]

But there can be no tock without a tick: Congress usually only strikes a better balance *after* the Court dramatically adjusts equilibrium, regardless of whether Fourth Amendment scholars deem it "error" or not. Indeed, it is ironic to call the Court's actions "equilibrium adjustment." Painting as it must in broad, doctrinal strokes,[72] the Court often supplies the greatest jolt of all because whatever general principle it announces to restore the status quo inevitably lacks the finer nuance that only a legislature, with its superior

63. *Id.* at 513.

64. *Id.* at 489.

65. *Id.* at 487–88.

66. *But see generally* Christopher Slobogin, Response, *An Original Take on Originalism*, 125 HARV. L. REV. F. 14, 14 (2011) (criticizing Kerr's equilibrium theory for resting on "shaky" "historical foundations," failing to explain past cases, and offering no meaningful guidance for today's hardest cases).

67. Kerr, *supra* note 61, at 531.

68. *Id.* at 539, 541.

69. 277 U.S. 438 (1928).

70. 389 U.S. 347 (1967); Kerr, *supra* note 61, at 539, 541–42.

71. Kerr, *supra* note 61, at 541.

72. Kerr describes this phenomenon as the interplay between the open-ended "principles layer" of Fourth Amendment doctrine with the "application layer," which produces seemingly arbitrary results when applied to specific facts. *Id.* at 490–91.

ability to gauge public attitudes, can provide.[73] Kerr's own example illustrates this pattern: just six years after the Supreme Court held in *Olmstead* that the Fourth Amendment did not bar wiretapping, Congress "corrected" the Court's "error" by passing the Communications Act, which made intercepting communications a federal crime.[74] And just *one* year after the Court's "correct" *Katz* decision, which held that the Fourth Amendment protects a person's reasonable expectation of privacy in their phone conversations,[75] Congress again "corrected" the Court by passing the Omnibus Crime Control and Safe Streets Act of 1968,[76] Title III of which (the "Wiretap Act") prescribed circumstances in which police *could* bug those conversations.[77]

As this Part will demonstrate, other Supreme Court ticks, both "positive" and "negative," have spurred Congress to act, whereas more recently, the careful judicial delay Kerr endorses has produced the same negative effects he ascribes to premature intervention: decades of legislative inaction and postponement of final, satisfactory answers to Fourth Amendment questions. Meanwhile, our rights continue to erode.

As the data broker loophole suggests, we have gone far too long without a tock. The Court has refused to strike with the blunt instrument of Fourth Amendment doctrine. Congress has sat idly by. And the clock has now struck thirteen. If we examine the pattern, however, we can learn from our mistakes, anticipate the striking of the Fourth Amendment clock, and chart a more promising path forward.

A. Congress Intervened to Correct the Court's "Positive" Equilibrium Adjustment in Katz

To determine whether the government needs a warrant to conduct a technological search, courts mainly look at whether the targeted individual

73. See Justice Alito's criticisms of judges using the "blunt instrument" of Fourth Amendment doctrine when public attitudes are still "in flux," discussed *infra* pp. 34–36. For a detailed discussion of competing perspectives on judicial versus legislative competence in Fourth Amendment decision-making, see Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 857–82 (2004). *But see* Daniel J. Solove, *Fourth Amendment Codification and Professor Kerr's Misguided Call for Judicial Deference*, 74 FORDHAM L. REV. 747, 773 (2005) ("In the context of crafting rules to regulate law enforcement and new technologies, I am not convinced that either the legislatures or the courts have strong advantages over the other.").

74. *Olmstead*, 277 U.S. at 464; Federal Communications Act of 1934, Pub. L. No. 73-416, 48 Stat. 1064, 1104 ("[N]o person not being authorized by the sender shall intercept any communication . . . .").

75. *Katz*, 389 U.S. at 353.

76. Pub. L. No. 90–351, 82 Stat. 197 (codified as amended in scattered sections of 18 and 34 U.S.C.).

77. *Id.* §801(b), 82 Stat. at 211–12, 216–18 (amending 18 U.S.C. §§ 2516–17 to set forth circumstances where wiretapping is authorized).

has a "reasonable expectation of privacy."[78] The reasonable expectation inquiry, derived from Justice Harlan's concurrence in *Katz*, asks two questions.[79] First, has the individual "exhibited an actual (subjective) expectation of privacy"?[80] And second, is that expectation "one that society is prepared to recognize as 'reasonable'"?[81] In *Katz*, the Court considered how Fourth Amendment doctrine should respond to the government's warrantless use of "an electronic listening and recording device" to eavesdrop on the defendant's conversation in a public phone booth.[82] *Tick*. The Court held that the government's use of this technology violated the defendant's reasonable expectation of privacy in "the words he utters into the mouthpiece" and that the government needed a warrant.[83] "To read the Constitution more narrowly," reasoned the Court, would "ignore the vital role that the public telephone has come to play in private communication."[84] *Tick*.

Congress responded the following year with the Omnibus Crime Control and Safe Streets Act of 1968—most notably Title III, commonly known as "the Wiretap Act,"[85] which authorizes the government to intercept communications under carefully prescribed circumstances.[86] Congress professed its desire to conform with *Katz*, but its real aim in passing the Wiretap Act was to "clarify the resulting confusion" caused by the Supreme Court, whose decisions had made the present state of surveillance law so "intolerable," serving "neither the interests of privacy nor of law enforcement," that both proponents and opponents of wiretapping agreed Congress must intervene.[87] As the Senate itself colorfully put it:

> It would be . . . difficult to devise a body of law from the point of view of privacy or justice more totally unsatisfactory in its consequences. . . . New protections for privacy must be enacted. Guidance and supervision must be given to State and Federal law

78. *See, e.g.*, United States v. Jones, 565 U.S. 400, 406 (2012) (summarizing the reasonable expectation of privacy standard); Fan, *supra* note 30, at 904 (same).

79. Smith v. Maryland, 442 U.S. 735, 740 (1979) (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

80. *Id.* (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

81. *Id.* (quoting *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

82. *Katz*, 389 U.S. at 348.

83. *Id.* at 352, 356–57.

84. *Id.* at 352. This is quintessential equilibrium-adjustment reasoning. Kerr, *supra* note 61, at 515.

85. *Title III of The Omnibus Crime Control and Safe Streets Act of 1968 (Wiretap Act)*, BUREAU OF JUST. ASSISTANCE, https://bja.ojp.gov/program/it/privacy-civil-liberties/authorities/statutes/1284 [https://perma.cc/Z5EX-U4CE].

86. S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

87. S. REP. NO. 90-1097, at 37–38 (1968), *as reprinted in* 1968 U.S.C.C.A.N. 2112, 2153–54.

> enforcement officers. *This can only be accomplished through national legislation.*[88]

How is that for an equilibrium adjustment? *Tock*.

B. Congress Intervened Again to Correct the Court's "Negative" Equilibrium Adjustment in Miller *and* Smith*—but Relied on the Court's False Dichotomy*

Before long, the Court had fashioned a carveout from its reasonable expectation of privacy test. Seizing on a caveat in *Katz* that "[w]hat a person knowingly exposes to the public, . . . is not a subject of Fourth Amendment protection,"[89] the Court in *United States v. Miller*[90] and later *Smith v. Maryland*[91] derived the "third-party doctrine": an individual generally lacks a reasonable expectation of privacy in information they provide to a third party, even if they reveal it "on the assumption[s] that it will be used only for a limited purpose" and that the third party will not "betray[]" that confidence.[92] Under the third-party doctrine, the government may freely obtain information shared with third parties without a warrant.[93]

Scholars have roundly criticized the third-party doctrine[94] as a serious threat to privacy in the digital age, in which people regularly expose information to countless companies in the ordinary course of business.[95] Even in 1986, years before the World Wide Web was introduced,[96] Congress recognized the third-party doctrine's disruptive potential in an increasingly interconnected world:

> With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal . . . information. . . . [B]ecause it is subject to control by a

88. *Id.* at 2156 (emphasis added).

89. *Katz*, 389 U.S. at 351.

90. 425 U.S. 435 (1976).

91. 442 U.S. 735 (1979).

92. *Miller*, 425 U.S. at 443; *see Smith*, 442 U.S. at 743–44 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties."); *see also* Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018) (reviewing the development of the third-party doctrine).

93. *See Carpenter*, 138 S. Ct. at 2216 (explaining that third-party information typically does not trigger Fourth Amendment protections).

94. See Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009), which colorfully captures scholars' criticism of the third-party doctrine as nothing less than "the *Lochner* of search and seizure law." Kerr ultimately defends the third-party doctrine, however, for "maintain[ing] the technological neutrality of Fourth Amendment rules" and "provid[ing] ex ante clarity." *Id.* at 564–65.

95. Solove, *supra* note 73, at 753; Fan, *supra* note 30, at 905–06.

96. *World Wide Web*, ENCYCLOPEDIA BRITANNICA, https://www.britannica.com/topic/World-Wide-Web [https://perma.cc/DLF9-H455].

> third party computer operator, the information may be subject to no constitutional privacy protection. See *United States v. Miller* . . . . Thus, the information may be open to possible wrongful use and public disclosure by law enforcement authorities . . . .[97]

To rebalance citizens' privacy with law enforcement's legitimate need for service provider data,[98] Congress passed the Electronic Communications Privacy Act of 1986,[99] which included the Stored Communications Act (SCA).[100]

Like the Wiretap Act, the SCA authorized the government to obtain certain private information under prescribed circumstances, depending on how sensitive Congress deemed the information to be.[101] Obtaining digital communications *contents* (e.g., email messages) without notifying the provider's customer requires a warrant, whereas obtaining certain *records* (e.g., name, address, or billing information) may only require a subpoena.[102] In 1994, Congress refined the balance by passing the Communications Assistance for Law Enforcement Act, which elevated the requirement for obtaining certain records to a court order.[103] Then, in 2001, Congress passed the USA PATRIOT Act, which amended the SCA to clarify that providers cannot "knowingly divulge" customer data "to any governmental entity" (except to prevent death or serious physical injury) but may freely divulge it to non-governmental entities.[104]

But these minor adjustments failed to fix the SCA's core issue: its illogical content–record dichotomy,[105] subconsciously lifted from *Katz*,

97. S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557.

98. *Id.*; Alan Z. Rozenshtein, *Fourth Amendment Reasonableness After* Carpenter, 128 YALE L.J.F. 943, 944 (2019); Isabelle Canaan, *A Fourth Amendment Loophole?: An Exploration of Privacy and Protection Through the Muslim Pro Case*, 6 COLUM. HUM. RTS. L. REV. ONLINE 95, 100–01 (2022).

99. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

100. Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1860 (1986) (codified as amended at 18 U.S.C. §§ 2701–11).

101. *Id.* §201, 100 Stat. at 1861–62; Rozenshtein, *supra* note 98, at 944–45.

102. Rozenshtein, *supra* note 98, at 945; 18 USC §§ 2703(a), 2703(b)(2)(A), 2703(c)(2).

103. Communications Assistance for Law Enforcement Act, Pub. L. No. 103–414, 108 Stat. 4279 (1994) (codified as amended at 47 USC §§ 1001–1010); H.R. REP. NO. 103–827(I), at 17 (1994), *as reprinted in* 1994 U.S.C.C.A.N. 3489, 3497. To justify this enhanced requirement, Congress pointed out that "society's patterns of using electronic communications technology have changed dramatically" in the intervening eight years since the Electronic Communications Privacy Act was passed, and that transactional records "reveal[] a great deal about [people's] private lives, all of it compiled in one place." *Id.*

104. USA Patriot Act of 2001, Pub. L. No. 107–56, 115 Stat. 272, 284–85 (codified as amended at 18 U.S.C. §§ 2702(a)(3), 2702(c)(4), 2702(c)(6)).

105. Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1288 (2004) (arguing lesser protection for records makes little sense when records can be "quite sensitive" and content "quite innocuous").

Miller, and *Smith*. As its name and enhanced protections for contents reflect, the Stored Communications Act contemplated the rise of new technologies for conveying messages—such as "electronic mail . . . cellular and cordless telephones, paging devices, and video teleconferencing."[106] But it failed to anticipate a future characterized by massive-scale record collection, in which data aggregated from smartphones, GPS devices, and other connected technologies might reveal more than a single phone conversation ever could. The Court had multiple opportunities to wield Fourth Amendment doctrine against these changes. But perhaps in a principled effort to avoid deciding too much too soon, the Court decided too little too late.

C. Jones *and* Riley *Exposed the Untenability of the Content–Record Dichotomy and the Court's Reluctance to Fix It*

Amid rapid, record-centric change, the Supreme Court began voicing concerns about the state of Fourth Amendment doctrine and what role the courts should play in privacy protection. In *United States v. Jones*,[107] the Court addressed whether the government's warrantless "attachment of a [GPS] tracking device" to the defendant's vehicle "to monitor the vehicle's movements on public streets" was a search or seizure under the Fourth Amendment.[108] At least superficially, one could scarcely imagine a better record-centric analog to *Katz*, which dealt with the warrantless attachment of "an electronic listening and recording device" to a phone booth to intercept the contents of the defendant's conversation.[109] But instead of wielding *Katz* to unwind the illogical content–record dichotomy by finding a reasonable expectation of privacy in records that reveal a person's precise movements, the majority dodged *Katz* entirely by leaning *backward* on the "degree of privacy against government that existed when the Fourth Amendment was adopted": protection from physical trespass.[110] The majority could have used *Jones* to tick but consciously chose not to.

Two competing views emerged in *Jones*'s disappointing wake. In her *Jones* concurrence, Justice Sotomayor acknowledged that GPS data, which precisely and comprehensively records a person's movements, reveals "a wealth of detail about [their] familial, political, professional, religious, and

106. S. REP. NO. 99-541, at 2 (1986), *reprinted in* 1986 U.S.C.C.A.N. 3555, 3556.

107. 565 U.S. 400 (2012).

108. *Id.* at 402.

109. Katz v. United States, 389 U.S. 347, 348 (1967).

110. *Jones*, 565 U.S. at 406 (quoting Kyllo v. United States, 533 U.S. 27, 34 (2001)). It speaks volumes about the Court's reluctance to address the third-party doctrine that Justice Scalia, rather than analogize to *Katz*, chose instead to compare the GPS device to an eighteenth-century constable "concealing himself in the target's coach." *Id.* at 406 n.3. Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan in his concurrence, ridiculed this analogy, pointing out that it "would have required either a gigantic coach, a very tiny constable, or both—not to mention a constable with incredible fortitude and patience." *Id.* at 420 n.3 (Alito, J., concurring).

sexual associations."[111] Without guardrails, the government's ability to aggregate such data was "susceptible to abuse."[112] Consequently, it might be time for the Court to "reconsider" the third-party doctrine, which was "ill[-] suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[113]

Or perhaps it was time for Congress—not the Court—to step in. In his *Jones* concurrence, Justice Alito observed that the reasonable expectation of privacy test assumes the "hypothetical reasonable person has a *well-developed and stable* set of privacy expectations."[114] However, in periods of dramatic technological change, popular attitudes about convenience–privacy tradeoffs may remain "in flux."[115] Whereas judges applying *Katz* might "confuse their own expectations of privacy with those of the hypothetical reasonable person," legislatures could effectively gauge changing public attitudes and draw "detailed lines" that more artfully balance citizens' privacy with public safety.[116] Indeed, after *Katz*, Congress had done just that: rather than "leave it to the courts" to adapt Fourth Amendment doctrine to the wiretap, Congress "promptly enacted a comprehensive statute" on the subject.[117] Neither Justice Sotomayor's nor Justice Alito's suggestion was heeded.

Two years later, in *Riley v. California*,[118] Chief Justice Roberts remarked that smartphones had become so pervasive that they were practically "an important feature of human anatomy."[119] Nodding to Justice Sotomayor's *Jones* concurrence, Chief Justice Roberts recognized smartphone data not only differed from physical records in sheer quantity but also qualitatively: searching through someone's browsing history, applications, and location data would reveal "the privacies of life," including "movements down to the minute."[120] Accordingly, a smartphone search might reveal "far more than the most exhaustive search of a house," and the government needed to obtain a warrant first.[121] But *Riley*'s holding, confined to searches incident to arrest and the cell phone itself, also failed to redress the core, underlying issue: the false content–record dichotomy.

111. *Id.* at 415 (Sotomayor, J., concurring).
112. *Id.* at 416.
113. *Id.* at 417.
114. *Id.* at 427 (Alito, J., concurring) (emphasis added).
115. *Id.*
116. *Id.* at 427, 429–30.
117. *Id.* at 427.
118. 573 U.S. 373 (2014).
119. *Id.* at 385.
120. *Id.* at 395–96, 403 (quoting in part Boyd v. United States, 116 U.S. 616, 630 (1886)).
121. *Id.* at 396, 403 (emphasis omitted).

Justice Alito, in his concurrence, reiterated that "it would be very unfortunate if privacy protection in the 21st century were left primarily to . . . courts using the blunt instrument of the Fourth Amendment."[122] Legislatures were still in a better position to adapt to technological change.[123]

But just because Congress should did not mean Congress would.

D. In Carpenter*, the Court Attempted—but Ultimately Failed—to Adjust Equilibrium*

In *Carpenter v. United States*, the Court had yet another chance to reconcile Fourth Amendment doctrine with sensitive third-party records.[124] *Carpenter* involved "cell-site location information": the time-stamped location data wireless carriers collect whenever a cell phone pings the network—even when their owners are not actively using them.[125] Prosecutors sought the cell-site location information of several robbery suspects, including the defendant Carpenter, from two wireless carriers via SCA court orders.[126] To meet the SCA's records standard, the prosecutors only needed to "offer[] specific and articulable facts showing . . . reasonable grounds to believe" the cell-site location information was "relevant and material to an ongoing criminal investigation."[127] The prosecutors requested seven days of cell-site location information from one carrier and 152 days from another, and they received two days and 127 days, respectively—"an average of 101 data points per day."[128] Using this data, they reconstructed Carpenter's movements, tying him to the scenes of four robberies.[129] Carpenter was convicted of multiple offenses and sentenced to over 100 years in prison.[130]

The Court held that Carpenter had a reasonable expectation of privacy in "the whole of [his] physical movements"[131] (at least across seven days[132]). His location data "was the product of a search," and the third-party doctrine did not excuse the government from having to secure a warrant for cell-site

122. *Id.* at 408 (Alito, J., concurring).

123. *Id.*

124. *See* 138 S. Ct. 2206, 2214–16 (2018) (reasoning that "personal location information maintained by a third party[] does not fit neatly under existing precedents").

125. *Id.* at 2211–12.

126. *Id.* at 2212.

127. *Id.* (quoting 18 U.S.C. § 2703(d)).

128. *Id.*

129. *Id.* at 2213.

130. *Id.*

131. *Id.* at 2217.

132. The Court declined to decide whether the government could acquire cell-site location information within some "cutoff" window (e.g., seven days) or how long such a window might be. *Id.* at 2217 n.3. It only held that "accessing seven days of [cell-site location information]" was definitively "a Fourth Amendment search." *Id.*

location information.[133] The Court reached these conclusions for three reasons.

First, the *comprehensiveness* of cell-site location information far exceeds most people's reasonable expectations about what the government may acquire through investigation. Using cell-site location information "in combination with other information," law enforcement can retroactively reproduce an "all-encompassing record" of any cell phone user's whereabouts for up to five years with almost GPS-level precision, "as if it had attached an ankle monitor to the phone's user."[134] The Court reasoned that this "near perfect surveillance" was a recent phenomenon that overwhelmed society's past expectations: prior to the digital age, such comprehensive surveillance was difficult, costly, rare, and "limited by a dearth of records and the frailties of [witnesses'] recollection."[135]

Second, the Court reasoned that cell-site location information *differs in kind* from information traditionally accessible via the third-party doctrine.[136] The *Miller* and *Smith* Courts "did not rely solely on the act of sharing" but also "considered 'the *nature* of the particular documents sought'" to determine whether a reasonable expectation of privacy arose.[137] And here, cell-site location information's "detailed chronicle" of a person's physical movements revealed far more than *Miller*'s checks or *Smith*'s call logs.[138]

Third, cell-site location information is "not truly 'shared'" by users; it leaves the cell phone "by dint of its operation, without any affirmative act on the part of the user beyond powering up" and with no way to opt out.[139] Accordingly, cell phone users do not "assume[] the risk" of transmitting their location data to a third-party carrier.[140]

The *Carpenter* Court took pains to emphasize, however, that its holding was "a narrow one" that did not address real-time collection of cell-site location information or "tower dumps,"[141] "conventional" surveillance techniques (e.g., security cameras), or "other business records that might incidentally reveal location information."[142] Confusingly, the Court insisted its holding did "not disturb the application of *Smith* and *Miller*" and declined

133. *Id.* at 2217.

134. *Id.* at 2217–19.

135. *Id.* at 2218–19.

136. *Id.* at 2219.

137. *Id.* (quoting United States. v. Miller, 425 U.S. 435, 442 (1976)) (emphasis added).

138. *Id.* at 2219–20.

139. *Id.* at 2220.

140. *Id.* (quoting Smith v. Maryland, 442 U.S. 735, 745 (1979)).

141. A tower dump is "a download of information on all the devices that connected to a particular cell site during a particular interval." *Id.*

142. *Id.*

to decide whether the government might constitutionally obtain *fewer* than seven days' worth of cell-site location information without a warrant.[143]

In other words, *Carpenter*, too, refused to tick. Vital time continued to slip away. The deep tilt of the police power–privacy scales threatened to become a new plane of equilibrium. Yet the Court—perhaps out of an admirable but anomalous desire to let Congress move first—remained largely mute.

IV. No, *Carpenter* and the Courts Will Not Save Us from Data Brokers

Carpenter has been hailed as "one of this generation's most important Fourth Amendment opinions."[144] Some have optimistically argued that its useful framework may save us from data brokers—at least when it comes to location data.[145] But *Carpenter* failed to answer several crucial Fourth Amendment questions. It will not save us from data brokers.

First, while *Carpenter*'s reasoning provides a useful framework for evaluating when certain data requires a showing of probable cause, the Court's holding is so narrow that it spoils its own application. In reaching its conclusion, the Court focused on three aspects of cell-site location information: its comprehensiveness, nature, and involuntary collection.[146] Some of the Court's dismissed alternatives appear to fit these criteria. Real-time collection of cell-site location information and "tower dumps," for example, would provide the same "ankle monitor"–like data as that provided by cell carriers, albeit for a shorter period. But the Court declined to consider whether or how time affected its analysis.[147] Law enforcement could easily collect the same mass of information by conducting *multiple* tower dumps—

143. *Id.*; *see supra* note 132.

144. *E.g.*, Rozenshtein, *supra* note 98, at 943; Taylor H. Wilson, Jr., Note, *The Mosaic Theory's Two Steps: Surveying* Carpenter *in the Lower Courts*, 99 TEXAS L. REV. ONLINE 155, 156 (2021) (collecting scholars' reactions).

145. *See generally* Rahbar, *supra* note 39 (arguing *Carpenter* applies beyond cell-site location information and bars government purchases of any involuntarily shared location data); *see* Canaan, *supra* note 98, at 116–17 (reasoning that because *Carpenter* was chiefly concerned with equilibrium adjustment and "the final possession of the information, rather than the specific process of acquisition," plaintiffs might challenge government data purchases under *Carpenter* itself).

146. *See supra* notes 134–43 and accompanying text.

147. *See supra* note 132. In *Sims v. State*, the Texas Court of Criminal Appeals addressed both questions, reasoning *Carpenter* applied to real-time cell-site location information but that "[w]hether a person has a recognized expectation of privacy . . . must be decided on a case-by-case basis." 569 S.W.3d 634, 645–46 (Tex. Crim. App. 2019). The court held that "less than three hours of real-time [cell-site location information] records" accessed by pinging a phone "less than five times" did *not* give rise to a reasonable expectation of privacy. *Id.* at 646. *But see* State v. Muhammad, 451 P.3d 1060, 1073 (Wash. 2019) (holding that cell phone users have a reasonable expectation of privacy in real-time cell-site location information, regardless of how long a "ping" lasts, because "[t]here is no rational point [in time at which] to draw the line").

across several days, several locations, or both.[148] Equally confounding, the Court stated its holding did "not disturb the application of *Smith* and *Miller*" or address "other business records that might incidentally reveal location information."[149] Consequently, it is unclear to what extent *Carpenter* applies beyond cell-site location information to other potentially sensitive records that data brokers sell.[150] For example, courts have consistently held that GPS data, which is more precise than cell-site location information, "fits squarely within the scope of the reasonable expectation of privacy."[151] But most courts have categorically held that an Internet user has no reasonable expectation of privacy in IP addresses,[152] which can also reveal the user's location or identity, albeit indirectly and with a few simple, additional steps.[153]

Second, *Carpenter* left unanswered the question of when a digital search begins, concluding only that a search had occurred: "[t]he location information obtained . . . was the *product* of a search."[154] The distinction matters because if *acquiring* data, as opposed to using it, does not count as a search, the government may freely purchase data from brokers without a warrant. Though the government might need a warrant at a later stage, if

148. *See* Jennifer Lynch, *Massachusetts' Highest Court Upholds Cell Tower Dump Warrant*, ELEC. FRONTIER FOUND. (May 27, 2022), https://www.eff.org/deeplinks/2022/05/massachusetts-highest-court-upholds-cell-tower-dump-warrant [https://perma.cc/A4X5-R4U8] (describing how police conducted tower dumps on "seven cell towers on seven different days over the course of a month," then "cross-referenced the tens of thousands of phone numbers they obtained" to identify one suspect).

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

150. *See, e.g.*, United States v. Trader, 981 F.3d 961, 967–68 (11th Cir. 2020) (characterizing *Carpenter*'s "'narrow' exception" as "apply[ing] only to some cell-site location information").

151. *E.g.*, United States v. Diggs, 385 F. Supp. 3d 648, 652 (N.D. Ill. 2019).

152. *See, e.g.*, United States v. Kidd, 394 F. Supp. 3d 357, 362–64 (S.D.N.Y. 2019) (collecting cases to show that "[e]very court to consider the application of *Carpenter* [to IP addresses] has declined to extend its reasoning" to that data). *But see* United States v. Taylor, 935 F.3d 1279, 1282, 1285 n.4 (11th Cir. 2019) (recognizing, without even mentioning *Carpenter*, that visitors to the "dark web" who use software to "purposefully shroud" their IP addresses have a reasonable expectation of privacy in that data).

153. *See Trader*, 981 F.3d at 968 ("Internet protocol addresses can be translated into location information only *indirectly*, by examining the internet company's business records to determine the physical address where the network is registered." (emphasis added)); *see* Matthew Hughes, *Can Law Enforcement Really Track Someone Down with an IP Address?*, HOW-TO GEEK (July 6, 2020), https://www.howtogeek.com/676872/can-law-enforcement-really-track-someone-down-with-an-ip-address [https://perma.cc/6P53-A5U4] (explaining that finding the Internet service provider associated with an IP address "is merely a matter of typing the IP address in the right [public] database," and that "[o]nce you've got the ISP, it's merely a matter of sending another subpoena").

154. *Carpenter*, 138 S. Ct. at 2217 (emphasis added). The Court has formulated Fourth Amendment issues this way before: in *Kyllo v. United States*, the Court held that information obtained via a thermal imager scan of the defendant's house was "the product of a search." 533 U.S. 27, 34–35 (2001).

history teaches us anything, it is that without clear *ex-ante* guidance, the government will not seek one.[155]

Professor Orin Kerr argues that the *Carpenter* Court did not reach the question of when a search begins because it implicitly relied on equilibrium-adjustment theory.[156] Round-the-clock surveillance by law enforcement used to be difficult and rare.[157] Cell phone technology and cell-site location information took that reasonable expectation away, giving the government "unlimited power to catalog" one's movements.[158] Consequently, the Court had to restore the traditional balance of police power by imposing a warrant requirement.[159] The question of when the search began or ended was irrelevant, which would explain why the Court equivocated between "access" and "acquisition" in describing the search.[160]

However, Justice Alito's and Justice Sotomayor's concurrences in *Jones* suggest a digital search may only begin after acquisition.[161] Justice Alito questioned whether people reasonably expect others to "secretly monitor *and catalogue*" their movements.[162] Justice Sotomayor similarly pondered whether people reasonably expect their movements "will be recorded *and aggregated*."[163] Kerr argues that because both Justices "looked beyond the initial data acquisition stage," some further action might be required (e.g., combining two datasets).[164] If Kerr is correct, the government's mere purchase and receipt of data from brokers would not

155. *See, e.g.*, Joseph Cox, *CBP Refuses to Tell Congress How It Is Tracking Americans Without a Warrant*, VICE: MOTHERBOARD (Oct. 23, 2020, 3:03 PM), https://www.vice.com/en/article/n7vwex/cbp-dhs-venntel-location-data-no-warrant [https://perma.cc/W3KT-3FWL] (describing how CBP failed to conduct a privacy impact assessment or obtain court orders before purchasing broker data, then cited attorney–client privilege in refusing to explain its legal reasoning to Congress).

156. Orin Kerr, *When Does a* Carpenter *Search Start—and When Does It Stop?*, LAWFARE (July 16, 2018, 10:24 AM), https://www.lawfareblog.com/when-does-carpenter-search-start-and-when-does-it-stop [https://perma.cc/T2YA-XFEP]; *see also* Kerr, *supra* note 61, at 487 (defining the equilibrium-adjustment theory).

157. Kerr, *supra* note 156; *see also supra* notes 134–35 and accompanying text.

158. Kerr, *supra* note 156.

159. *Id.*

160. *Id.* For example, the government "invaded Carpenter's reasonable expectation of privacy" when it "*accessed* [cell-site location information] from the wireless carriers," but "[t]he [g]overnment's *acquisition* of the cell-site records was a search." *Id.* (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219–20 (2018)) (emphasis added).

161. *Id.*

162. *Id.* (quoting United States v. Jones, 565 U.S. 400, 430 (2012) (Alito, J., concurring)).

163. *Id.* (quoting *Jones*, 565 U.S. at 416 (Sotomayor, J., concurring)).

164. *Id.* (citing Orin S. Kerr, *The Mosaic Theory of the Fourth Amendment*, 111 MICH. L. REV. 311, 332 (2012)).

violate the Fourth Amendment. The government could then kick the probable cause can down the road—into court, after the harm occurred.[165]

Third, *Carpenter* may preserve what Kerr calls the "willing seller rule": a person relinquishes all Fourth Amendment rights in an item when they voluntarily sell it in the ordinary course of business.[166] Kerr deduces this rule from the Supreme Court's decision in *Maryland v. Macon*,[167] which found no Fourth Amendment seizure occurred when an undercover agent purchased "obscene" magazines from a store clerk "in the ordinary course of business" because the clerk had "voluntarily transferred any possessory interest he may have had . . . upon the receipt of the funds."[168] Before *Carpenter*, Kerr explains, the government could clearly purchase data without running afoul of the Fourth Amendment; a database seller would surrender its Fourth Amendment rights to data the moment funds changed hands, and the subject of the data would never have had a reasonable expectation of privacy in the first place under the third-party doctrine.[169]

Carpenter changed the calculus slightly by providing that, at least in some contexts, individuals have a reasonable expectation of privacy in third parties' records about them, and compelling a company to produce those records may be a Fourth Amendment search.[170] Under the willing-seller rule, then, a data broker might not have authority to extinguish an individual's coequal Fourth Amendment rights in records about them—unless a court applies the doctrine of "third-party consent": when multiple people have Fourth Amendment rights in an item, any person with joint control may consent to a government search.[171] The government could argue that the willing-seller rule and third-party consent create a one-two punch: by voluntarily selling data in the ordinary course of business, the broker forfeits its Fourth Amendment rights *and* those of the subject because the broker, who had joint control, could consent to a government search. *Carpenter*'s framework fails to address the willing-seller rule or third-party consent.[172] Even assuming *Carpenter* might extend beyond its narrow holding, from

165. Even if, in the short term, the government fails to convince a court that *Carpenter* does not apply to data acquired from brokers, it may still succeed in using such data at trial by showing it *reasonably relied* on *Carpenter*'s binding precedent at the time. *See* Davis v. United States, 564 U.S. 229, 241 (2011) ("Evidence obtained during a search conducted in reasonable reliance on binding precedent is not subject to the exclusionary rule."). On remand, not even Carpenter himself could escape this exception. United States v. Carpenter, 926 F.3d 313, 317–18 (6th Cir. 2019).

166. Orin S. Kerr, *Buying Data and the Fourth Amendment*, HOOVER INST. 3–4 (November 17, 2021) (Aegis Series Paper No. 2109), https://www.hoover.org/sites/default/files/research/docs/kerr_webreadypdf.pdf [https://perma.cc/G5DW-3UX2].

167. 472 U.S. 463 (1985).

168. Kerr, *supra* note 166, at 2 (quoting *Macon*, 472 U.S. at 469, 471).

169. *Id.* at 2–3.

170. *Id.* at 3.

171. *Id.* at 4.

172. *Id.* at 4–5.

cell-site information to other sensitive digital records, a lower court might still feel compelled to apply the willing-seller rule and third-party consent, which are at least thirty years older than *Carpenter* and not cabined to specific facts.[173]

Fourth, relying on litigants alone to extend *Carpenter* would be inefficient. Courts rule against criminal defendants "in the overwhelming majority (specifically, four out of five) of Fourth Amendment cases."[174] A variety of factors might account for this. Criminal defendants are often "unsympathetic, . . . litigate[] bad facts," and "rarely [have] access to a good lawyer."[175] Moreover, because criminal defendants often fail to "present courts with relevant statistics" to help courts weigh law enforcement's conduct against citizens' privacy, courts may engage in "blind balancing"—frequently against the defendant.[176] Assuming a criminal defendant could afford an appeal, it may take as long as two years to get a decision.[177] Inevitable variations and splits within and among jurisdictions will also hinder the development of more predictable post-*Carpenter* case law.

Although it offers a promising framework, *Carpenter* will not save us from data brokers. Congress must act.

V. Congress Must Close the Fourth Amendment Loophole with New Privacy Legislation

The time has come for Congress to "tock" and pass new privacy legislation to close the SCA's glaring Fourth Amendment loophole. As in 1986, today's law is "hopelessly out of date."[178] It has "not kept pace with the development" of smartphones and other constantly connected record-keeping devices.[179] We no longer have time to "leave it to the courts to develop a body of Fourth Amendment case law."[180] Just as Congress balanced citizens' privacy with legitimate law enforcement need for

173. *See generally Macon*, 472 U.S. 463 (1985) (finding no Fourth Amendment seizure occurred when an undercover agent purchased obscene material because the clerk had voluntarily sold the material); United States v. Matlock, 415 U.S. 164 (1974) (holding that officers did not violate the Fourth Amendment when they obtained consent from a third party who had authority over the property).

174. Ryan Calo, *Can Americans Resist Surveillance?*, 83 U. CHI. L. REV. 23, 36 (2016).

175. *Id.*

176. *Id.* (quoting in part Shima Baradaran, *Rebalancing the Fourth Amendment*, 102 GEO. L.J. 1, 3 (2013)).

177. *How Long Do Federal Appeals Take?*, SHEIN, BRANDENBURG & SCHROPE: FED. CRIM. L. CTR., https://federalcriminallawcenter.com/frequently-asked-questions/how-long-do-federal-appeals-take [https://perma.cc/XB9M-LQGQ].

178. S. REP. NO. 99-541, at 2 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556 (quoting 132 CONG. REC. 14600 (1986) (statement of Sen. Patrick Leahy)).

179. *Id.*

180. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring).

wiretapping after *Katz*, then accessing digital information after *Smith* and *Miller*,[181] Congress must now prescribe circumstances under which the government may purchase data from brokers.

Although Congress has considered other potential privacy legislation,[182] the proposed Fourth Amendment Is Not for Sale Act[183] and My Body, My Data Act[184] illustrate two promising federal approaches. California's recently enacted data broker-focused privacy law, S.B. 362, colloquially known as the "Delete Act,"[185] also provides a compelling, state-level model that Congress might wish to develop and federalize. I propose my own legislative solution, in the original spirit of the SCA, which would incorporate the strengths of all three.

A. The Fourth Amendment Is Not for Sale Act: Procedural Safeguards

The Fourth Amendment Is Not for Sale Act, first proposed in 2021 and reintroduced in 2023,[186] would solve the Fourth Amendment loophole with *procedure*: who may access third-party data and how. The Act would amend the SCA's existing framework to prohibit law enforcement or intelligence agencies from obtaining third-party records or "illegitimately obtained information" "in exchange for anything of value"—regardless of who obtained, collected, or disclosed it first.[187]

---

181. *See* S. REP. NO. 99-541, at 2–3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3556–57 (describing how Congress enacted electronic privacy laws in response to *Katz* and *Miller*).

182. *E.g.*, American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022). *But see* Hayley Tsukayama, Adam Schwartz, India McKinney & Lee Tien, *Americans Deserve More Than the Current American Data Privacy Protection Act*, ELEC. FRONTIER FOUND. (July 24, 2022), https://www.eff.org/deeplinks/2022/07/americans-deserve-more-current-american-data-privacy-protection-act [https://perma.cc/D3WU-FJ7A] (arguing that the proposed ADPPA would impede privacy law enforcement by agencies, "ha[ve] no teeth" via private enforcement, and give too much leeway to companies that collect or process information for the government).

183. Fourth Amendment Is Not for Sale Act, S.2576, 118th Cong. (2023).

184. My Body, My Data Act of 2023, H.R. 3420, 118th Cong. (2023).

185. Act of Oct. 10, 2023, ch. 709 (codified at Cal. Civ. Code §§ 1798.99.80–.82, 1798.99.84–.87, 1798.99.89 (2023)); Tracy Shapiro, Eddie Holman & Doo Lee, *California Enacts One-Stop Mechanism for Data Broker Deletion Requests*, WILSON SONSINI (Oct. 25, 2023), https://www.wsgr.com/en/insights/california-enacts-one-stop-mechanism-for-data-broker-deletion-requests.html [https://perma.cc/5MNW-TRZU].

186. Press Release, Ron Wyden, U.S. Sen., Wyden, Paul and Bipartisan Members of Congress Introduce The Fourth Amendment Is Not for Sale Act (Apr. 21, 2021), https://www.wyden.senate.gov/news/press-releases/wyden-paul-and-bipartisan-members-of-congress-introduce-the-fourth-amendment-is-not-for-sale-act- [https://perma.cc/7ATP-57T5]; Press Release, Bipartisan Senators Reintroduce the Fourth Amendment Is Not for Sale Act, *supra* note 7.

187. Fourth Amendment Is Not for Sale Act, S. 2576, 118th Cong. § 2 (2023) (proposing to amend 18 U.S.C. by adding § 2702(e)(2)). Covered records include those "collected by a third party" or disclosed by a "provider" or "intermediary service provider." *Id.* (proposing to amend 18 U.S.C. by adding § 2702(e)(1)(A)). It does not matter whether the third party was the first to collect the record, just that the record was collected by a third party at some prior point. *Id.* (proposing to

The Fourth Amendment Is Not for Sale Act protects broad swaths of data, including information directly "linked" to someone's identity and anonymized data "that, if combined with other information, could be used to identify a person."[188] In addition to records traditionally covered by the SCA, the Fourth Amendment Is Not for Sale Act singles out "location information" for protection: anything "derived or otherwise calculated from the transmission or reception of a radio signal that reveals" someone's "approximate or actual geographic location."[189] This definition implicates cell-site location information but also GPS data.[190] Although nothing stops governmental entities *outside* law enforcement and intelligence from buying third-party records from brokers, the Fourth Amendment Is Not for Sale Act prohibits these entities from sharing purchased data with law enforcement or intelligence, which would circumvent the Act's procedural safeguards.[191]

Moreover, the Fourth Amendment Is Not for Sale Act does not just graft the SCA's existing record requirements onto third-party data requests. To request information from a third party, the government must follow "the most stringent standard under Federal statute *or the Constitution*" that a court would otherwise use to evaluate a court order to a provider for comparable information.[192] This provision's reference to the Constitution leaves open the possibility that, for some data types, the Constitution may require the government to meet a higher standard, and it invites rather than prescribes courts' judgment. Any third-party information obtained in violation of the Fourth Amendment Is Not for Sale Act is inadmissible in "any trial, hearing, or other proceeding."[193]

However, the Fourth Amendment Is Not for Sale Act leaves a few stones unturned. Its exclusive focus on exchanges "for anything of value" creates another loophole: data brokers could *give* information to law

amend 18 U.S.C. by adding § 2702(e)(2)(B)). Accordingly, a data broker that acquires records from *another* data broker could not claim its data is exempt. "[I]llegitimately obtained information" means records a provider obtains in ways inconsistent with its own policies or that otherwise "deceiv[e]" the customer. *Id.* (proposing to amend 18 U.S.C. by adding § 2702(e)(1)(E)). To "obtain in exchange for anything of value" means to receive (1) by purchase, (2) "in connection with services being provided for consideration," or (3) "otherwise . . . in exchange for consideration" such as access or licensing fees. *Id.* (proposing to amend 18 U.S.C. by adding § 2702(e)(1)(H)).

188. *Id.* (proposing to amend 18 U.S.C. § 2702 by adding § 2702(e)(1)(J)).

189. *Id.* (proposing to amend 18 U.S.C. § 2702 by adding § 2702(e)(1)(C)(ii)–(iii) and § 2702(e)(1)(G)).

190. *How Does GPS Work?*, NASA: SPACEPLACE (June 27, 2019), https://spaceplace.nasa.gov/gps/en [https://perma.cc/G2P9-MCDH] ("A GPS receiver in your phone listens for . . . signals. Once the receiver calculates its distance from four or more GPS satellites, it can figure out where you are.").

191. Fourth Amendment Is Not for Sale Act, S.2576, 118th Cong. § 2 (2023) (proposing to amend 18 U.S.C. § 2702 by adding § 2702(e)(3)).

192. *Id.* § 3 (proposing to amend 18 U.S.C. § 2703 by adding § 2703(i)(3)(B)) (emphasis added).

193. *Id.* § 2 (proposing to amend 18 U.S.C. § 2702 by adding § 2702(e)(4)).

enforcement for free—perhaps to avoid regulatory scrutiny or to obtain government contracts.[194] And individuals have no information about or control over how their data is shared; at most, they may bring a civil action against a data broker only after the harm is complete.[195] Lastly, no federal agency has authority to enforce the Fourth Amendment Is Not for Sale Act or craft data-sharing rules that adapt to changing technology.

B. The My Body, My Data Act: Categorical Data Protection

The My Body, My Data Act, first proposed in 2022 and reintroduced in 2023,[196] closes the Fourth Amendment loophole with categorical *data protection*—for "personal reproductive or sexual health information"[197] (PRSHI data). Unlike the Fourth Amendment Is Not for Sale Act, which amends and relies on multiple Electronic Communications Privacy Act sections, the My Body, My Data Act was written from the ground up to operate almost exclusively within its own airtight universe. It governs four groups: individuals, regulated entities, agents (employees and service providers), and third parties.[198] Regulated entities essentially include any person, business, or nonprofit not already covered by HIPAA or the Public Health Service Act.[199] By default, a regulated entity may not "collect, retain, use, or disclose" any PRSHI data; it may only do so when "strictly necessary to provide a product or service" the individual requested.[200] Even then, the regulated entity may only grant PRSHI data access to agents "for which

194. Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying It.*, BRENNAN CTR. FOR JUST. (Apr. 28, 2021), https://www.brennancenter.org/our-work/analysis-opinion/government-cant-seize-your-digital-data-except-buying-it [https://perma.cc/8FXB-HY8R]*; see also, e.g.*, Cyphers, *supra* note 44 (describing data brokers' strategy of giving their product away to earn goodwill with public health officials as "COVID-washing"). Closing this loophole, on the other hand, might prevent third parties from *voluntarily* assisting with government investigations except in case of emergency. *See* 18 U.S.C. § 2702(c)(4) (permitting disclosure of customer records to the government if the provider has a good-faith belief that an emergency involving death or serious injury so requires).

195. The First Amendment Is Not for Sale Act leaves in place 18 U.S.C. § 2707(a), which permits "any . . . person aggrieved by any violation of [the SCA]" to sue a "person or entity, other than the United States," who knowingly or intentionally violated the SCA.

196. Press Release, Congresswoman Sara Jacobs, *supra* note 24.

197. My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 2(a) (2023).

198. *Id.* §§ 2(b), 6(b)(1), 7(6)–(8).

199. *Id.* § 7(6).

200. *Id.* § 2(a). The original My Body, My Data Act (of 2022) would have also allowed PRSHI data collection and use with an individual's "express consent," but this exception was omitted from the 2023 bill. *Compare* My Body, My Data Act of 2022, H.R. 8111, 117th Cong. § 2(a)(1) (2022) (allowing a regulated entity to collect PRSHI data "with the express consent of the individual"), *with* My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 2(a) (2023) (omitting "express consent" provision). The bill's sponsors may have felt that even an "express" consent requirement was too easily gamed via lengthy terms of service, deceptive user interfaces, and other tricks to obtain users' "voluntary" consent.

access is necessary" to provide that product or service.[201] Data brokers and other third parties without a service role are shut out.

The My Body, My Data Act provides extensive data protection in three ways. First, all terms are broadly and inclusively defined. Protected data may relate to an individual's "past, present, or future reproductive or sexual health," including data in seven highly detailed categories.[202] It need not even *directly* identify an individual—just "relate[] to, describe[], [be] reasonably capable of being associated with, or . . . reasonably be linked, directly or indirectly" with an individual, their household, or one of their devices.[203] To "collect" and "disclose" include "*any* manner" of obtaining or divulging data, respectively.[204] Because the Act grants the Federal Trade Commission rulemaking authority,[205] the agency may further particularize these definitions.

Second, the My Body, My Data Act informs individuals and gives them control over their data. A regulated entity must "prominently publish" a privacy policy on its website that "clear[ly] and conspicuous[ly]" describes the kinds of data it collects; which "specific third parties" it has shared data with or obtained data from and why; how it uses and protects that data; and how an individual may exercise control over the data associated with them.[206] Upon request, an individual may access, correct, or delete PRSHI data—including data that third parties collected or even "*inferred*" about that individual—and receive a list of specific third parties with whom the regulated entity has shared that data, all within fifteen days and free of charge.[207]

Lastly, the My Body, My Data Act has teeth. The FTC would enforce it,[208] and "[a]ny individual" alleging a violation may bring a civil action.[209] Violators may face FTC penalties,[210] or if an individual plaintiff prevails, an award of the *greater* of actual damages or up to $1000 per day, in addition to punitive damages, costs, and reasonable attorney's fees.[211] A regulated entity may not retaliate against an individual for exercising control over data, and

201. My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 2(b) (2023).
202. *Id.* § 7(5).
203. *Id.* § 7(4).
204. *Id.* § 7(1), (3).
205. *Id.* § 6(a)(3).
206. *Id.* § 4(a)–(c).
207. *Id.* § 3(a)–(c), 3(d)(2)–(3) (emphasis added).
208. *Id.* § 6(a). *But see The U.S. Urgently Needs a Data Protection Agency*, ELEC. PRIV. INFO. CTR., https://epic.org/campaigns/dpa [https://perma.cc/TV8T-WFKE] (criticizing the FTC for failing thus far to adequately protect personal data).
209. My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 6(b)(1) (2023).
210. *Id.* § 6(a)(2).
211. *Id.* § 6(b)(2).

any arbitration agreement or joint-action waiver covering disputes arising under the Act will be invalidated.[212]

Although it prescribes virtually everything else, unlike the Fourth Amendment Is Not for Sale Act, the My Body, My Data Act does not prescribe procedures for obtaining PRSHI data legitimately; regulated entities may still divulge PRSHI data to the government in "compliance with a court order."[213] Moreover, the My Body, My Data Act's protection, though extensive, is limited to a single data category.

C. The "Delete Act": A Tailored State-Level Solution

California's newest privacy law, S.B. 362, colloquially known as the "Delete Act,"[214] features many of the My Body, My Data Act's robust data protections but is specifically tailored to data brokers. First, its "personal information" definition is equally broad as—indeed, nearly identical to—that of the My Body, My Data Act.[215] However, the Delete Act extends data protection to all such personal information—not just PRSHI data—and grants rulemaking authority to an agency focused exclusively on data protection issues: the California Privacy Protection Agency.[216]

Second, the Delete Act, like the My Body, My Data Act, gives individuals visibility and control over how brokers use their data. Data brokers must host webpages that explain the types of information they collect, sell, or share and to whom; how state residents may correct or delete data associated with them; and how they may limit or opt out of future data sharing.[217] By 2026, data brokers must also offer an "accessible deletion mechanism," to be hosted on the California Privacy Protection Agency's

212. *Id.* § 6(b)(4)(A).

213. *Id.* § 10.

214. *See supra* note 185 and accompanying text.

215. *Compare* CAL. CIV. CODE § 1798.140(v)(1) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household," including information in twelve enumerated categories), *with* My Body, My Data Act of 2023, H.R. 3420, 118th Cong. § 7(4) (2023) (defining "personal information" as "information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular individual, household, *or device*") (emphasis added); *see also* Act of Oct. 10, 2023, ch. 709, § 1(a) (adopting the "personal information" definition from CAL. CIV. CODE § 1798.140(v)(1) into the Delete Act). Representative Jacobs no doubt used her home state's existing privacy laws as a baseline for the My Body, My Data Act.

216. *See* Act of Oct. 10, 2023, ch. 709, § 9 (declaring that the Delete Act will protect Californians from having their personal information collected by data brokers); Cal. Civil Code § 1798.99.87(a) (granting authority to the CPPA); *Frequently Asked Questions (FAQs)*, CAL. PRIV. PROT. AGENCY, https://cppa.ca.gov/faq.html#faq_cppa_2_body [https://perma.cc/748P-E66R].

217. CAL. CIV. CODE § 1799.82(b)(2)(G)(i). These sites must also be free of "dark patterns": website designs intended to trick individuals into taking actions, like sharing data, that they did not intend. *Id.* § 1799.82(b)(2)(G)(ii); *see generally What Are Deceptive Patterns?*, DECEPTIVE PATTERNS, https://www.deceptive.design [https://perma.cc/X2KW-ABVB].

website, permitting residents to submit a "single verifiable consumer request" to all registered data brokers (and, by extension, their service providers and contractors) to opt out, selectively delete data, or delete all their associated data within forty-five days—and every forty-five days going forward—free of charge.[218] If a deletion request cannot be executed, the Delete Act requires brokers to cease sharing the requester's data by default.[219]

Lastly, the Delete Act, like the My Body, My Data Act, has teeth. Any data broker who holds the personal information of a California resident—even just *one*—must register with and pay fees to the California Privacy Protection Agency or risk administrative fines (up to $200 per day) and costs in an action brought by the agency.[220] Registered data brokers must notify the agency upfront whether it collects precise geolocation data, "reproductive health care data," or minors' personal information;[221] regularly report deletion requests and other metrics to the agency; and, beginning in 2028, undergo audits every three years.[222] Brokers who fail to execute a deletion request on time will be fined $200 per request per day until they comply.[223] Because nearly 40 million people call California home, the cost of noncompliance might quickly become crippling.[224]

But the Delete Act does not fully explore every avenue. It requires brokers who collect "precise geolocation" and "reproductive health care data" to report this fact to California's agency in advance, suggesting these categories are especially significant. Yet, unlike the Fourth Amendment Is Not for Sale Act and the My Body, My Data Act, respectively, the Delete Act does not single out either category for enhanced protection, and it leaves "reproductive health care data" undefined.[225] Because the Delete Act lacks a

218. CAL. CIV. CODE § 1798.99.86(a)–(c), 1798.99.86(d)(1)–(2).

219. *Id.* § 1798.99.86(c)(1)(B).

220. *Id.* § 1798.99.82(b)(1), (c); Shapiro, Holman & Lee, *supra* note 185. The Act excludes entities already regulated under the Fair Credit Reporting Act, Gramm-Leach-Bliley Act, California's Insurance Information and Privacy Protection Act, and HIPAA. CAL. CIV. CODE §§ 1798.99.80(c)(1)–(4), 1798.146.

221. CAL. CIV. CODE § 1798.99.82(b)(2)(C)–(E).

222. *Id.* §§ 1798.99.85, 1798.99.86(e).

223. *Id.* § 1798.99.82(d)(1).

224. *See* Shapiro, Holman & Lee, *supra* note 185 (explaining that, if just one percent of state residents submitted deletion requests, the Delete Act could impose fines of "$80 million *per day*" on data brokers). But for the most profitable data brokers, steep fines might not sufficiently deter noncompliance. Rob Shavell, *Why California's 'Delete Act' Matters*, FORBES (Sept. 5, 2023, 6:15 AM), https://www.forbes.com/sites/forbestechcouncil/2023/09/05/why-californias-delete-act-matters/?sh=6c7da16012f5 [https://perma.cc/3TTG-GUTJ].

225. Instead, the Delete Act treats all broker data equally under California's version of the Electronic Communications Privacy Act. *Compare* CAL. CIV. CODE § 1798.99.86(c)(2)(A) (excusing brokers from deleting data on request when maintaining it is "reasonably necessary . . . to fulfill a purpose described in subdivision (d) of Section 1798.105"), *with id.* § 1798.105(d)(5)

private cause of action, residents cannot hold non-compliant brokers accountable themselves; they must trust that the California Privacy Protection Agency will do it for them—a needlessly risky bet.[226] Worse, data brokers may avoid deleting any "deidentified" data,[227] even though studies show one can easily reidentify up to 95% of individuals with as few as four data points.[228]

Even so, the Delete Act is a solid starting point. By 2026, the data of nearly 40 million Americans[229] may be removed from the open market—and consequently from warrantless government purchases. The two-year lead gives the California legislature ample time to close loopholes.[230] And just as California's general data protection law, the California Consumer Privacy Act, inspired eight other states to enact their own data protection laws, the Delete Act may spur Texas, Oregon, and Vermont, who have already passed data broker registration laws, and other states to adopt broker-specific restrictions modeled after the Delete Act.[231] As state restrictions overlap and contradict each other, Congress may intervene with a national standard, using the Delete Act as a baseline.[232]

(listing as one such purpose "[compliance] with the California Electronic Communications Privacy Act"). Though the Act does not define "reproductive health care data," it *does* define "precise geolocation": "any data . . . derived from a device . . . intended to be used to locate a consumer within a geographic area . . . with a radius of 1,850 feet." *Id.* § 1798.140(w).

226. Shapiro, Holman & Lee, *supra* note 185.

227. *See* CAL. CIV. CODE § 1798.99.86(c)(2)(B) ("[A] data broker shall not be required to delete a consumer's personal information if . . . deletion is not required pursuant to Section 1798.145 . . . ."); *id.* § 1798.145(a)(1)(F) (exempting from obligation entities that "[c]ollect, use, retain, sell, share, or disclose consumers' personal information *that is deidentified*") (emphasis added). More fundamentally, "personal information" excludes "deidentified" information: "information that cannot reasonably be used to infer information about, or otherwise be linked to, a particular consumer" so long as the covered entity "[t]akes reasonable measures" to ensure it remains deidentified, refrains from reidentifying it, and contractually obligates recipients to comply. *Id.* § 1798.140(v)(3), 1798.140(m). These voluntary obligations will not curb abuse.

228. Lomas, *supra* note 15.

229. Shapiro, Holman & Lee, *supra* note 185.

230. Though it equally gives lobbyists ample time to walk back restrictions. *See* Titus Wu, *Californians Get Stronger Deletion Rights Against Data Brokers*, BLOOMBERG L. (Oct. 10, 2023, 4:01 PM), https://www.bloomberglaw.com/product/blaw/bloomberglawnews/ip-law/BNA 0000018a-b4fd-d37f-a7ae-b6fd2334000c [https://perma.cc/NW7L-5WD5] (quoting advertising group's complaint that "[g]iven the glaring and dramatic failures in the [Delete Act], the only good news is that there are more than two years until it goes into effect, so the legislature has time to return to this issue . . . [and] act on the critical fixes needed").

231. Kirk J. Nahra, Ali A. Jessani & Samuel Kane, *Texas and Oregon Adopt New Rules for Data Broker Laws*, WILMERHALE (Dec. 14, 2023), https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/20231214-texas-and-oregon-adopt-new-rules-for-data-broker-laws [https://perma.cc/6VUT-Y223]; Shavell, *supra* note 224.

232. Shavell, *supra* note 224.

D. My Proposal: The New Spirit of Carpenter *Act*

I propose a more effective Fourth Amendment cure—the New Spirit of *Carpenter* Act (New SCA)—that would learn from the past. Like the SCA, the New SCA would balance legitimate law enforcement needs with privacy interests.[233] It would update and clarify these standards in light of today's technological innovations, combining the Fourth Amendment Is Not for Sale Act's procedural strengths with the My Body, My Data Act's and Delete Act's data protections.[234] But unlike the SCA, it would provide enough flexibility to keep pace with the technological developments of tomorrow.[235]

First, the New SCA would authorize legitimate government access in prescribed circumstances, depending on the data's sensitivity. The SCA relied on false dichotomies. It imposed special rules for obtaining information from providers but said nothing about third parties.[236] In our digital age, "people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks."[237] If not from providers, law enforcement can seek equally sensitive or even more revealing records from third parties, as it has from data brokers. No sound reason remains for treating providers differently. Under the New SCA, *all* third-party records would, regardless of their source, receive at least the same level of protection initially afforded by the SCA.

Moreover, the SCA falsely assumed that records deserved less protection than contents.[238] But certain records, when aggregated, are qualitatively different,[239] revealing *more* than the contents of our communications, such as our "familial, political, professional, religious, and sexual associations"[240] or other "privacies of life."[241] These records accordingly merit the same enhanced protection as communications contents.[242] Chief Justice Roberts identified at least three stand-out categories

---

233. *See* S. REP. NO. 99-541, at 3 (1986), *as reprinted in* 1986 U.S.C.C.A.N. 3555, 3557 (discussing the need for balance between "privacy interests in personal and proprietary information" and "the Government's legitimate law enforcement needs").

234. *See id.* at 1 (describing the SCA as "updat[ing] and clarify[ing] Federal privacy protections and standards in light of dramatic changes in new computer and telecommunications technologies").

235. *See id.* at 2 (lamenting that pre-SCA laws failed to keep "pace with changes in the structure of the telecommunications industry").

236. *See* 18 U.S.C. § 2703 (only outlining procedures for governmental entities to require disclosure "by a *provider*" of electronic communication or remote computing services) (emphasis added).

237. United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring).

238. *See supra* notes 107–08 and accompanying text.

239. Riley v. California, 573 U.S. 373, 395–96 (2014).

240. *Jones*, 565 U.S. at 415 (Sotomayor, J., concurring).

241. *Riley*, 573 U.S. at 403 (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).

242. *See* Solove, *supra* note 105, at 1286–88 (arguing that "the distinction between content and envelope information does not correlate well to the distinction between sensitive and innocuous information").

in *Riley*: location data (physical movements), browsing history (digital movements, often collected without consent[243]), and health information.[244] California's Delete Act identified a fourth: *minors'* personal information.[245] Like the Fourth Amendment Is Not for Sale Act and the My Body, My Data Act, the New SCA would broadly define each special data category. And like the Fourth Amendment Is Not for Sale Act, it would also require law enforcement to meet "the most stringent standard under Federal statute or the Constitution" to obtain access to this data.[246]

Second, the New SCA would appropriately balance access with privacy interests. Privacy today is *contextual*. We entrust third parties with our data "on the assumption that it will be used only for a limited purpose" and that they will not "betray[]" our confidence.[247] We realize such purposes may include targeted advertising—sometimes facilitated by broker data—when a service is free. But we do not, by sharing alone, assume the risk of "unrestrained search[es] for evidence of criminal activity"[248] by law enforcement; we properly expect the Fourth Amendment to stand in the way. To restore balance, we need three things: (1) *information* about how our data has been and will be used so we may provide informed consent; (2) *control* over our data, including the ability to access, correct, or delete it within a reasonable time; and (3) *power* to hold those who break the rules accountable. The New SCA would amend the Electronic Communications Privacy Act to require providers and intermediaries[249] to maintain and display privacy policies that inform users about how their data is used. It would give users control over their data by adopting the My Body, My Data Act's strict protections for location data, browsing data, health data, and minors' data.[250] To empower individuals and punish violators, the New SCA would include

243. *See, e.g.*, Harry Guinness, *Cookies Are Going Away, But Internet Tracking May Still Be Here to Stay*, POPULAR SCI. (Apr. 21, 2022, 7:00 PM), https://www.popsci.com/technology/cookies-internet-tracking [https://perma.cc/L5DA-87N7] (explaining that even as tech companies block third-party cookies, making it harder to track users *across* apps and services, many will still track users' actions *within* their ecosystems via account-based methods).

244. *See Riley*, 573 U.S. at 395–96 (specifically identifying, among other things, "[h]istoric location information," "Internet search and browsing history," and "apps for tracking pregnancy symptoms").

245. *See supra* note 223.

246. Fourth Amendment Is Not for Sale Act, S.2576, 118th Cong. § 3 (2023) (proposing to amend 18 U.S.C. § 2703 by adding § 2703(i)(3)(B)).

247. Smith v. Maryland, 442 U.S. 735, 744 (1979) (quoting United States v. Miller, 425 U.S. 435, 443 (1976)).

248. *Riley*, 573 U.S. at 403.

249. The Fourth Amendment Is Not for Sale Act defines "intermediary service provider" as "an entity or facilities owner or operator that directly or indirectly delivers, stores, or processes communications for or on behalf of a provider . . . ." Fourth Amendment Is Not for Sale Act, S.2576, 118th Cong. § 4 (2023).

250. *See supra* notes 204–14 and accompanying text.

a private cause of action, and liable third parties would risk punitive damages and other costs.

Third, the New SCA would remain adaptable to emerging technologies. We cannot, as Congress did in enacting the SCA, mistakenly assume data's sensitivity will remain stagnant while collection and analysis tools improve. The New SCA would grant enforcement and rulemaking power to a federal agency—perhaps the FTC or a dedicated data protection agency[251]—to take pressure off courts, who must otherwise apply old doctrines to entirely new industries. By learning from past mistakes, the New SCA would anticipate the ticking of the Fourth Amendment clock, ensuring it never strikes thirteen again.

Conclusion

Since at least the 1920s, Fourth Amendment doctrine and statutory privacy protections have largely followed a tick–tick–*tock* cycle. Some revolutionary technology emerges. Law enforcement, recognizing its surveillance potential, exploits the technology without obtaining a warrant. *Tick*. The Supreme Court acknowledges the technology's increased importance to participation in modern society and creates a hardline cutoff—leaving the technology entirely inside or outside Fourth Amendment protection. *Tick*. Congress, seeking to strike a more delicate balance between legitimate government access and individual privacy, intervenes to clarify appropriate scenarios in which the government may use the technology for surveillance. *Tock*. *Katz*'s reasonable expectation of privacy test, the Wiretap Act, *Smith* and *Miller*'s third-party doctrine, and the Electronic Communications Privacy Act (including the Stored Communications Act) all owe their existence to this cycle.

However, as the post-*Dobbs* data-sharing panic and renewed scrutiny of data brokers illustrates, we have gone too long without a "tock" from Congress. The Communications Assistance for Law Enforcement Act and USA PATRIOT Act's minor revisions to the Stored Communications Act failed to eliminate the SCA's outmoded content–record dichotomy in response to paradigm technological shifts. Justices' opinions in *Jones* and *Riley* exhibited an increasing discomfort in applying existing Fourth Amendment doctrine to prolific GPS and smartphone records. In *Carpenter*, this concern boiled over: drawing from *Jones* and *Riley*, the Court narrowly excluded cell-site location information from the third-party doctrine because it was more comprehensive, different in kind, and "not truly shared" by users.

251. *See The U.S. Urgently Needs a Data Protection Agency*, *supra* note 208 (advocating for an independent, federal data protection agency in light of the FTC's failure to adequately protect personal data).

Scholars have rightly hailed *Carpenter* as a potential turning point in Fourth Amendment doctrine and digital data, but it will not save us from government surveillance through data brokers. *Carpenter*'s holding is explicitly narrow and difficult to apply consistently to other records. It fails to clarify when a digital search begins and ends, a question essential to whether the government's mere purchase and receipt of data from brokers without a warrant violates the Fourth Amendment. Even courts that apply *Carpenter* liberally face the willing-seller rule and the doctrine of third-party consent. And relying on litigants and courts alone to iron out Fourth Amendment inconsistencies will take—and has already taken—far too long. If we continue to shrug off and normalize government infringement of our Fourth Amendment rights, we risk losing them forever. We must not fall backward into the same world of generalized searches and unchecked surveillance that the Fourth Amendment was intended to eliminate. The clocks are striking thirteen. It is time for Congress to "tock" and pass new privacy legislation now.

In striking a new balance between legitimate government access and individual privacy, Congress must learn from its past mistakes and draw from the procedural and data protection advantages illustrated by the proposed Fourth Amendment Is Not for Sale Act and My Body, My Data Act, as well as California's new Delete Act. Congress must abolish false dichotomies—between content and records and between providers and third parties. It must recognize, as the *Carpenter* Court did, that some data is qualitatively different, revealing far more than communication contents or even the search of a house. Congress should define these data types and afford them enhanced protection. It must acknowledge that today's privacy is contextual and that individuals accordingly need information about how their data is used, control over its use, and power to hold their data stewards accountable. Lastly, Congress must ensure that the new legislation remains flexible in the face of future technological development.

That way, when the Fourth Amendment clock strikes again, we will be ready.