Catholic University Law Review

Volume 73
Issue 3 *Summer 2024*

Article 9

7-1-2024

Dude, Where's My Data? A Legislative Band-Aid for Data Brokers' Bullet Hole in Consumer Privacy Protection

Emily Bushman

Dude, Where's My Data? A Legislative Band-Aid for Data Brokers' Bullet Hole in Consumer Privacy Protection

Cover Page Footnote

J.D. Candidate, May 2024, The Catholic University of America, Columbus School of Law.

DUDE, WHERE'S MY DATA? A LEGISLATIVE BAND-AID FOR DATA BROKERS' BULLET HOLE IN CONSUMER PRIVACY PROTECTION

Emily Bushman[+]

The development and proliferation of the Internet, GPS, cell phones, social media, and the associated data that support these now ubiquitous technologies have created a new ecosystem of information making up a person's digital identity. Our digital footprints have traditionally been subject to different levels of privacy protection depending upon the kind of data at issue. Over time, court decisions have revealed tensions and a lack of consistency on the question of how the protections guaranteed by the Fourth Amendment apply to an individual's digital footprint and their reasonable expectations of privacy over it. This Comment will examine the gaps in the current landscape of U.S. privacy protections in the absence of federally explicit legislative protections. First, it will examine current federal statutory privacy law and the piecemeal approach through which certain areas of information or categories of individuals are protected. Next, it will examine the development of the Supreme Court's Fourth Amendment jurisprudence as applied to individual privacy rights. It will then analyze the gaps in privacy protection in both statutory and case law and recommend a unified federal statutory approach to ensure that currently legal uses of data do not, when aggregated, yield an impermissibly intrusive infringement of the privacy rights of U.S. citizens in violation of the spirit of the Fourth Amendment's protections. It will recommend a legislative solution to fill those gaps, provide a clear expression of how certain kinds of data can and cannot be used, and ensure these critical protections are applied equally to all, regardless of the state in which any individual lives.

[+] J.D. Candidate, May 2024, The Catholic University of America, Columbus School of Law.

INTRODUCTION 500
I. PRIOR LAW 502
A. Statutory Protections 502
1. State by State 502
2. Federal Law 502
B. Case Law Development–Interpreting our Right to Privacy 505
1. Reasonable Expectation of Privacy and Trespass Doctrine 505
2. Third-Party Doctrine 506
3. Carpenter and its Updates 511
a. Carpenter's Impact? 512
b. What Even Is My Data? 512
II. ANALYSIS 515
A. Statutory Gaps 515
1. State Gaps 515
2. Federal Gaps 516
B. Gaps in Case Law and Litigation 518
1. Third-Party Doctrine Issues 518
2. Carpenter Issues: Scope, Time, and Data Type 518
III. COMMENT 519
A. Dude, Now What? 519
B. Criticisms 521
CONCLUSION 522

INTRODUCTION

"Right now, and I mean this instant, delete every digital trace of any menstrual tracking. Please."[1] Reverberations from the Supreme Court's decision in *Dobbs v. Jackson Women's Health* overturning *Roe v. Wade* extended beyond the initial physical impact on women. Suddenly, with a new focus, the fissures in American privacy protections in the digital sphere were exposed. Many individuals began to realize how much of their information is shared with the apps, websites, and platforms they interact with daily, and the scope of the picture that could be gleaned when that information is aggregated from these disparate sources and considered in its entirety. This Comment is not focused on privacy issues related specifically to abortion rights and their exercise. Rather, this Comment focuses on the fact that American citizens have limited federal data privacy protections, at times in conflict with state-level protections, and those federal protections are riddled with gaps and exceptions (of which the holding in *Dobbs* and its impact on digital traces of reproductive access and care are just the latest examples).[2] As the amount of information available about each of us continues to proliferate and its uses expand, it is increasingly urgent that the problems and gaps in the current approach to and analysis of privacy protections be addressed.

The Fourth Amendment to the U.S. Constitution provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[3] The development and proliferation of the Internet, GPS, cell phones, social media, and the

---

1. @ginasue, TWITTER (June 24, 2022, 11:10 AM), https://twitter.com/ginasue/status/1540354137304760321?ref_src=twsrc%5Etfw%7Ctwcamp%5Etweetembed%7Ctwterm%5E1540354137304760321%7Ctwgr%5E93173d0268491a820ed77fab5d907bf2d5436082%7Ctwcon%5Es1_&ref_url=https%3A%2F%2Fwww.nytimes.com%2F2022%2F06%2F30%2Ftechnology%2Fperiod-tracker-privacy-abortion.html [https://perma.cc/52GY-4HBC].

2. Recently, the Washington Post broke a story in which a private Denver-based nonprofit organization that privately sought and purchased social media application's tracking data for users. The organization, Catholic Laity and Clergy for Renewal, was able to effectively purchase the identifying information of priests who used "gay dating and hookup apps" and then distributed that information nationally to bishops. Michelle Boorstein & Heather Kelly, *Catholic Group Spent Millions on App Data That Tracked Gay Priests*, WASH. POST (Mar. 9, 2023, 8:52 AM), https://www.washingtonpost.com/dc-md-va/2023/03/09/catholics-gay-priests-grindr-data-bishops/ [https://perma.cc/8UVW-GMK3]. As will become clear throughout this Comment, the troubling nature of this acquisition and distribution is its absolute legality. Nothing in the process of obtaining, purchasing, or distributing this location data to others is against U.S. law. *Id.* Beyond the initial data privacy concerns for individual users, there are additional layers of the organization being a private group, not a state actor, precluding the potential application of the Fourth Amendment of this potential data "search." Even if the Fourth Amendment would apply, the First Amendment would likely preclude these identified priests from seeking relief for action taken against them by the Church. *See* Hosanna-Tabor Evangelical Lutheran Church v. EEOC, 565 U.S. 171, 174–75, 196 (2012); Our Lady of Guadalupe Sch. v. Morrissey-Berru, 591 U.S. 732, 736, 756 (2020).

3. U.S. CONST. amend. IV.

associated data that support these now ubiquitous technologies have created a new ecosystem of information making up a person's digital identity. Our digital footprints have traditionally been subject to different levels of privacy protection depending upon the kind of data at issue. As our digital presence becomes increasingly interconnected and decreasingly optional, a closer look at the way data privacy is protected is warranted.

At the time of the founding, the prevailing idea of privacy was that "every man's home [was] his castle" and that intrusion into that space was a serious matter that required the utmost care.[4] A warrant was needed, "particularly describing the places to be searched, and the persons or things to be seized," to justify state intrusion into the one place a person could reasonably expect to enjoy privacy.[5] As technology has advanced, information that would be found in someone's "houses, papers, and effects" has moved from physical items and documents to intangible pieces of data, and is now located not only in their own homes but in their personal devices, in their text messages and messaging apps, and in data centers all over the world.[6]

Over time, court decisions have revealed tensions and a lack of consistency on the question of how the protections guaranteed by the Fourth Amendment apply to an individual's digital footprint and their reasonable expectations of privacy over it. A more centralized understanding would help. Considering the Fourth Amendment's original purpose was to allow a man's home to be his castle, it may be time, through federal legislation, to expand the understanding and intention of that Amendment to protect digital castles as well.

This Comment will examine the gaps in the current landscape of U.S. privacy protections in the absence of federally explicit legislative protections. First, it will examine current federal statutory privacy law and the piecemeal approach through which certain areas of information or categories of individuals are protected. Next, it will examine the development of the Supreme Court's Fourth Amendment jurisprudence as applied to individual privacy rights. It will then analyze the gaps in privacy protection in both statutory and case law and recommend a unified federal statutory approach to ensure that currently legal uses of data do not, when aggregated, yield an impermissibly intrusive infringement of the privacy rights of U.S. citizens in violation of the spirit of the Fourth Amendment's protections. It will recommend a legislative solution to fill those gaps, provide a clear expression of how certain kinds of data can and cannot be used, and ensure these critical protections are applied equally to all, regardless of the state in which any individual lives.

---

4. Laura Hecht-Felella, *The Fourth Amendment in the Digital Age*, BRENNAN CTR. FOR JUST. 1, 4 (Mar. 18, 2021), https://www.brennancenter.org/our-work/policy-solutions/fourth-amendment-digital-age [https://perma.cc/TF6G-GP59].

5. U.S. CONST. amend. IV.

6. *Id.*

I. PRIOR LAW

At the federal level, U.S. law protects data privacy in two ways: through statutes, which typically either narrowly apply to a specific kind of data, a specific type of individual, or a specific agency that has jurisdiction over certain functions, and through case law invoking the Fourth Amendment.[7]

A. Statutory Protections

1. State by State

States offer their own forms of statutory protections, with varying levels of comprehensiveness and specificity. Currently, only California and Virginia have comprehensive statutes in effect protecting consumer privacy, and these laws only apply to individuals within those states.[8] Colorado, Connecticut, and Utah enacted statutes that took effect in 2023. Colorado and Connecticut have recently enacted comprehensive statutes that took effect on July 1, 2023, while Utah's took effect on December 31, 2023.[9] Many states have or are considering some intermediate level of statutory protection, including states with bills in committee or covering specific areas of data, like eBook privacy (Missouri) or covering biometric data (Illinois).[10] This patchwork state-by-state approach leaves individuals with varying protections of privacy over the same information depending on where they live.

2. Federal Law

Federal protections for data are similarly varied, but generally apply to a specific kind of information. In the past, this approach may have been adequate as the technological advances and changes in information technology were not as rapid or dynamic, and the concept of consumer digital privacy had not yet solidified. The statutes in place in the United States are targeted to cover specific kinds of data and are widely viewed as outdated in the context of modern

---

7. Thorin Klosowski, *The State of Consumer Data Privacy Laws in the US (And Why It Matters)*, N.Y. TIMES (Sept. 6, 2021), https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/ [https://perma.cc/N7XB-KTU6]; *see, e.g.*, Carpenter v. United States, 585 U.S. 296 (2018).

8. Klosowski, *supra* note 7. Some critics note that even the comprehensive state laws still fall short of actual consumer privacy protection, noting that Virginia's law, for example, is business-friendly, relies on opt-out consent, and was heavily influenced by Amazon throughout its drafting.

9. Colorado and Connecticut's statutes took effect July 1, 2023, and Utah's took effect December 31, 2023. *State Laws Related to Digital Privacy*, NAT'L CONF. OF STATE LEGISLATURES (June 7, 2022), https://www.ncsl.org/technology-and-communication/state-laws-related-to-digital-privacy#:~:text=Five%20states%E2%80%94California%2C%20Colorado%2C,of%20personal%20information%2C%20among%20others [https://perma.cc/3ENN-X8J2].

10. Klosowski, *supra* note 7.

information technology.[11] Legislation specific to particular kinds of data and the ways in which that data can be accessed or used includes the Gramm-Leach-Bliley Act (GLBA), Health Insurance Portability and Accountability Act (HIPPA), the Fair Credit Reporting Act (FRCA), the Family Educational Rights and Privacy Act (FERPA), the Children's Online Privacy Protection Act (COPPA), the Video Privacy Protection Act (VPPA), the Computer Fraud and Abuse Act (CFAA), and the Consumer Financial Protection Act (CFPA).[12] None of these, with the exception of the FCRA, specifically focus on the current marketplace of consumer data, and have remained fairly effective at protecting the narrow areas of information they were drafted to cover.

Similarly, agencies with congressionally delegated jurisdiction over certain types of activities also issue administrative rules and regulations and have established protections that govern specific arenas and the data in them. These include the Federal Communications Commission (FCC), the Securities and Exchange Commission (SEC), and the Federal Trade Commission (FTC).[13]

From a broader federal statutory perspective, data privacy laws have not been comprehensively updated since the Electronic Communications Privacy Act (ECPA) was passed in 1986.[14] The ECPA has "three acts: the Wiretap Act, the Stored Communications Act, and the Pen Register Act."[15] The intent of the ECPA is to apply protections to communications data and to extend the reach of Fourth Amendment-like protections, especially aimed at law enforcement.[16] Because the ECPA is not specifically aimed at any one sector, it is generally considered the most extensive and comprehensive federal data privacy protection available.[17] However, it is also widely considered outdated, as it has not been amended to specifically reflect the emergence of the consumer-centered Internet and associated data collection or to reflect the vast amounts of data captured by smartphones and the apps that run on them.[18] Although some

11. *See id.*

12. *Id.*; STEPHEN P. MULLIGAN & CHRIS D. LINEBAUGH, CONG. RSCH. SERV., R45631, DATA PROTECTION LAW: AN OVERVIEW 7–36 (2019).

13. MULLIGAN & LINEBAUGH, *supra* note 12, at 14–19, 21–23.

14. Elizabeth Goitein, *The Government Can't Seize Your Digital Data. Except by Buying it.*, WASH. POST (Apr. 26, 2021), https://www.washingtonpost.com/outlook/2021/04/26/constitution-digital-privacy-loopholes-purchases/ [https://perma.cc/RB3E-EXAD]. For more information on the relationship between the commercial use of data and users' privacy, *see* Jake Holland, *Facebook Data Release to Cops Evades Fourth Amendment Limits*, BLOOMBERG L. (Apr. 29, 2022), https://news.bloomberglaw.com/privacy-and-data-security/facebook-data-release-to-cops-evades-fourth-amendment-limits; Stephanie Comstock Ondrof, Comment, *"Senator, We Run Ads": Advocating for a US Self-Regulatory Response to the EU General Data Protection Regulation*, 28 GEO. MASON L. 815 (2021); Ignacio N. Cofone & Adriana Z. Robertson, *Consumer Privacy in a Behavioral World*, 69 HASTINGS L. J. 1471 (2018).

15. Electronic Communications Privacy Act of 1986, Pub. L. No. 99–508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2510–2523); MULLIGAN & LINEBAUGH, *supra* note 12, at 25.

16. MULLIGAN & LINEBAUGH, *supra* note 12, at 25.

17. *Id.*

18. *Id.*

plaintiffs have sought to extend the ECPA to cover the commercial use of consumer data gleaned from online activity, these cases have largely been unsuccessful, as the ECPA was intended to focus on things like wiretapping and has not been construed by courts to extend to commercial data gathering and collection.[19]

The state of communications has seismically changed since the passage of the ECPA nearly forty years ago, with cell phones and social media radically changing the amount of information sent between people daily and the amount of data supporting those communications held by private companies. This lack of protection of commercially generated and held data encroaches upon the government context when law enforcement agencies purchase data from private companies to use in investigations without users knowing that their information is being obtained and reviewed by the government.[20]

Congress attempted to pass legislation to update statutory protections of privacy but has thus far failed. Its most recent attempt is the American Data Privacy Protection Act (ADPPA),[21] which received some attention from a House committee during the 117th Congress.[22] It remains to be seen whether it will be re-introduced in the current 118th Congress.[23] Other bills introduced in Congress include the Government Surveillance Transparency Act of 2022,[24] the Warrant for Metadata Act,[25] the Fourth Amendment Is Not For Sale Act,[26] and the Email Privacy Act.[27] None passed in the 117th Congress (which ended in

19. *Id.* In contrast, the European approach to privacy regulations take a significantly wider approach in the General Data Protection Regulation (GDPR) which begins to take effect whenever any entity, government, public, or private, begins to aggregate substantial amounts of data. *Id.* at 40.

20. *See* Goitein, *supra* note 14.

21. American Data Privacy and Protection Act (ADPPA), 117 H.R. 8152, 117th Cong. (2022).

22. Former Speaker, Nancy Pelosi, had indicated in 2022 that she will not bring a vote on the ADPPA until it mirrors the strength of California's data privacy protections. *Pelosi Statement of Federal Data Privacy Legislation*, U.S. HOUSE OF REPRESENTATIVES (Sept. 1, 2022), https://pelosi.house.gov/news/press-releases/pelosi-statement-on-federal-data-privacy-legislation [https://perma.cc/H7GS-Z353]; JONATHAN M. GAFFNEY ET AL., CONG. RSCH. SERV., LSB10776, OVERVIEW OF THE AMERICAN DATA PRIVACY AND PROTECTION ACT, H.R. 8152, at 1 (2022), https://crsreports.congress.gov/product/pdf/LSB/LSB10776 [https://web.archive.org/web/20240616013336/https://crsreports.congress.gov/product/pdf/LSB/LSB10776].

23. As of press time, it has still not been introduced. Arlo Gilbert, *Federal Privacy News: Is the ADPPA Back?*, OSANO (Mar. 2, 2023), https://www.osano.com/newsletter/federal-privacy-news-is-the-adppa-back [https://perma.cc/DV92-8N6K].

24. Government Surveillance Transparency Act of 2022, S. 3888, 117th Cong. (2022); Government Surveillance Transparency Act of 2022, H.R. 7214, 117th Cong. (2022).

25. Warrant for Metadata Act, H.R. 7553, 117th Cong. (2022).

26. Fourth Amendment Is Not For Sale Act, H.R. 2738, 117th Cong. (2022).

27. Email Privacy Act, H.R. 8961, 116th Cong. (2020).

January 2023).[28] However, the Fourth Amendment Is Not For Sale Act was reintroduced in the 118th Congress and was passed by the House on April 17, 2024.[29]

B. Case Law Development–Interpreting our Right to Privacy

1. Reasonable Expectation of Privacy and Trespass Doctrine

The Fourth Amendment provides, "The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated."[30] At the time of the founding, the prevailing notion of privacy was that "a man's home was his castle" and that intrusion into that space was a serious matter that could not be lightly justified.[31] A warrant was needed that "particularly describ[ed] the place to be searched, and the persons or things to be seized" to justify state intrusion into the one place a person could reasonably expect to enjoy privacy.[32]

This geographic, location-based understanding of the Fourth Amendment broke down with *Katz v. United States*. *Katz* advanced the understanding that privacy protections under the Fourth Amendment apply to situations beyond the traditional "trespass doctrine," or the idea that the Fourth Amendment applies only to invasions of a physical space, or a trespass.[33] *Katz* expanded the search jurisprudence to include those actions that did not involve an in-person search or physical trespass but involved an electronic listening device outside a phone booth. The Supreme Court held that this conduct amounted to a search that had occurred in violation of the Fourth Amendment.[34] In *Katz*, the Court determined "[f]or the first time [that] the Fourth Amendment protections were divorced from the physical trespass requirement."[35] This also led to the "*Katz* test," holding that "the Constitution protects against government intrusion when a person has

---

28. S. 3888; H.R. 7214; H.R. 7553; Fourth Amendment Is Not For Sale Act, S. 1265, 117th Cong. (2021); H.R. 2738; H.R. 8961.

29. Fourth Amendment Is Not For Sale Act, H.R. 4639, 118th Cong. (2024). The bill now heads to the Senate, and if passed, will require signature by the President. The Biden Administration has commented negatively on the bill, arguing that the Act will undercut U.S. national security objectives and capabilities to interdict drug trafficking and other important national interests, though the administration as refrained on announcing whether or not it will veto. David DiMolfetta, *House passes bill barring spy agencies, law enforcement from buying Americans' personal data*, NEXTGOV FCW (Apr. 18, 2024), https://www.nextgov.com/cybersecurity/2024/04/house-passes-bill-barring-spy-agencies-law-enforcement-buying-americans-personal-data/395830/#:~:text=The%20House%20of%20Representatives%20on,commercial%20providers%20like%20data%20brokers [https://perma.cc/EVV6-ZH4V].

30. U.S. CONST. amend. IV.

31. Hecht-Felella, *supra* note 4, at 4.

32. U.S. CONST. amend. IV.

33. Hecht-Felella, *supra* note 4, at 4; Katz v. United States, 389 U.S. 347, 353 (1967).

34. Hecht-Felella, *supra* note 4, at 4; *Katz*, 389 U.S. 347.

35. Hecht-Felella, *supra* note 4, at 4; *Katz*, 389 U.S. at 353.

exhibited an actual ([or] subjective) expectation of privacy and their expectation of privacy is one that society is objectively prepared to recognize as reasonable."[36] The *Katz* extension of the Fourth Amendment to any kind of monitoring or surveillance, regardless of physical trespass, was critical to the substantial advancement of Fourth Amendment jurisprudence.[37]

As technology has developed, the kinds of information that would be found in someone's "houses, papers, and effects"[38] has moved from primarily physical documentation to digital records and is now located, not only in their own home, but in the data stored on devices. These technological developments have outpaced the application of the trespass doctrine and have begun to chafe against the next major development in Fourth Amendment jurisprudence, the "third-party doctrine."

2. Third-Party Doctrine

Under *Katz*, the Court began to ask where exactly it is that individuals can have a "reasonable expectation of privacy."[39] One recurring question is whether individuals can have a reasonable expectation of privacy in information that they have voluntarily shared with a third-party. So, for example, while under *Katz*, an individual has a reasonable expectation that the government will not be tapping their telephone call with a business associate (so a warrant is required to tap that call), there is no requirement for law enforcement to get a warrant to separately talk to the business associate about the content of that telephone call. This is termed the "third-party doctrine," which establishes "that individuals have no legitimate expectation of privacy in information they voluntarily share with third parties, regardless of whether or not they intended for the government to have access to that data."[40] This means that "while the government would need a warrant to obtain an individual's personal papers from their home, law enforcement could obtain the same papers from a third party with whom they had been shared—even for a limited purpose—with little to no legal process."[41] This doctrine was formally codified by *United States v. Miller* and *Smith v. Maryland*.[42]

In *Miller*, the defendant had shared personal information with his bank, and the Court held that "Miller had no legitimate expectation of privacy in his financial records . . . because he had 'voluntarily conveyed' this information to a third party."[43] The Court found it was of no consequence that Miller gave

36. Hecht-Felella, *supra* note 4, at 4 (citing *Katz*, 389 U.S. at 361 (Harlan, J., concurring)).

37. Hecht-Felella, *supra* note 4, at 4; *Katz*, 389 U.S. at 353.

38. U.S. CONST. amend. IV.

39. Hecht-Felella, *supra* note 4, at 4.

40. *Id.*

41. *Id.* at 5.

42. *Id.* at 4; *see* Smith v. Maryland, 442 U.S. 735, 740 (1979); United States v. Miller, 425 U.S. 435, 437 (1976).

43. Hecht-Felella, *supra* note 4, at 5; *Miller*, 425 U.S. at 442–43.

those records and information to the third-party as a requirement for doing business with the bank; all that was necessary was that Miller had voluntarily disclosed the information to a third-party, which meant the government did not need a warrant to access it.[44] In *Smith*, the Court also found "law enforcement's use of a pen register, a device installed by a telephone company at its offices to monitor the telephone numbers dialed on defendant Michael Smith's home phone, was not a search requiring a warrant."[45] To reach this conclusion, the Court determined that Smith "voluntarily assumed the risk that the phone company might relay the numbers he called to the police."[46] Of note for future jurisprudential developments, in his dissent Justice Marshall questioned how voluntary these disclosures actually were considering that "disclosure to a third-party bank or phone carrier is not truly voluntary, given that banks and phones are necessary components of modern society."[47]

The major dispute for current courts is the extent to which data can realistically be considered "voluntarily shared" by the user.[48] Things like location data, Wi-Fi access, server access, and other forms of data are "shared" each time an individual uses a computer, sends a text message, or accesses a social media application. While there is still a range between technological uses that are virtually required to engage meaningfully in modern daily life and those that are still optional, that range is shrinking.[49] The amount of information that

---

44. Hecht-Felella, *supra* note 4, at 5; *Miller*, 425 U.S. at 440–43.

45. Hecht-Felella, *supra* note 4, at 5; *Smith*, 442 U.S. at 740, 742. Note that the pen register is now an outdated form of technology, but was once deemed important enough to warrant specific language in the ECPA. Electronic Communications Privacy Act of 1986 § 101(4) (codified as amended at 18 U.S.C. § 2511(2)(h)). Questions remain about how relevant this specific technology is in modern use cases, and further indicate the datedness of the ECPA. However, it could be a relevant consideration as courts evaluate other like kinds of data and databases for evaluation in terms of privacy protections and criminal investigations. *See* Jane Bambauer, *Letting Police Access Google Location Data Can Help Solve Crimes*, WASH. POST (Mar. 28, 2022), https://www.washingtonpost.com/outlook/2022/03/28/geofence-warrant-constitution-fourth-amendment/ [https://perma.cc/T8EJ-NS54] (asserting that while there are valid privacy concerns in the vast amount of assembled location data held by tech companies, the reasonable expectations of privacy of users are still relevant in considering a potential broach of the Fourth Amendment).

46. Hecht-Felella, *supra* note 4, at 5; *Smith*, 442 U.S. at 744–46.

47. Hecht-Felella, *supra* note 4, at 5; *Smith*, 442 U.S. at 749–50.

48. *See, e.g.*, *Carpenter*, 585 U.S. 296.

49. For example, just four years ago, TikTok did not exist. While the short video social network poses a variety of national security concerns based on its parentage ownership interests, those are beyond the scope of this article. What is worth noting about the app is the distinction it draws in comparison to other tools. Some may argue that TikTok is another social network, and not required for meaningful participation in daily life. Therefore, because it is still an optional network, it falls well short of the requirements to meaningfully engage in life that, say, web search or Internet access carries. While that may be true for the time being, there are those who work through social networks in small businesses and gain market share by word of mouth for their business and products, and the virality of being seen by TikTok's algorithm expands potential business. It may be easy for some to say TikTok is an optional platform, but those who are self-employed in this way likely would argue the opposite. If TikTok and email are too divergent, once

can be aggregated to create a complete digital footprint of an individual user is rapidly increasing.[50] This information is then excluded from privacy protections under the third-party doctrine, which means that law enforcement officials can obtain the information from that third-party, either through a subpoena or, in some cases, by purchasing it.[51] A developing issue is when use of (practically speaking) non-optional digital technologies creates, via "knowing exposure" and purchase, a circumvention of constitutional privacy protections from unreasonable, warrantless searches.[52]

An additional facet of third-party doctrine emerged through examining the reasonable expectations of privacy individuals have while in public, as opposed to private, spaces.[53] Two cases were especially critical in drawing the distinction between public movements and a person's reasonable expectation of privacy.[54] In *United States v. Knotts*, the Court held that law enforcement personnel, who attached a beeper to Knotts' car, did not need a warrant to track "[a] person traveling in an automobile on public thoroughfares."[55] Because the defendant, Knotts, had traveled on public roads, law enforcement could have gained the same location and tracking information had they followed him in person (as opposed to utilizing the technological advancement of the beeper), and Knotts, therefore, had no reasonable expectation of privacy in his comings and goings.[56] In *United States v. Karo*, the Court drew a major distinction between public and private spaces and determined that while the use of a beeper in Knotts' car to track movements on public roads was permissible, it would be an unconstitutional overstep for the government to use a beeper to track an individual's activity inside their homes, where there is a reasonable expectation of privacy.[57]

The distinction in these cases remains essential as new technological advancements blur the line between public movements and private behavior.

---

you start walking away from the poles and toward the center, it becomes much blurrier. Is an Instagram required? Or Facebook? A Twitter account? These are still social networks that help monitor businesses and products and engage with consumers. Is a website required? There is no bright line, making evaluation of the problem complicated.

50. *See generally*, FED. TRADE COMM'N, DATA BROKERS: A CALL FOR TRANSPARENCY AND ACCOUNTABILITY vii (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/9NVX-FLJ4].

51. Hecht-Felella, *supra* note 4, at 4.

52. Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*," THE BRENNAN CTR. FOR JUST., (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole [https://perma.cc/P8GT-A6XZ].

53. Hecht-Felella, *supra* note 4, at 5.

54. *Id.*; *see, e.g.*, United States v. Knotts, 460 U.S. 276, 281, 285 (1983); *see also* United States v. Karo, 468 U.S. 705, 716 (1984).

55. Hecht-Felella, *supra* note 4, at 5; *Knotts*, 460 U.S. at 281, 285.

56. Hecht-Felella, *supra* note 4, at 5; *Knotts*, 460 U.S. at 281–82.

57. Hecht-Felella, *supra* note 4, at 5; *Karo*, 468 U.S. at 716.

The Court's reasoning raised an important dividing line: the use of surveillance technology to monitor activity in places that are not typically able to be visually surveilled (as a public street or throughway is) triggers heightened constitutional protections, as there is a strong expectation of privacy in those areas.[58] This distinction is especially important as technology continues to advance. For example, in *Florida v. Riley*, the Court determined that the defendant Riley did not have a reasonable expectation of privacy in his exterior greenhouse on his property because it was visible from above, and the debated surveillance occurred from a plane using aerial views.[59]

The debate about what constitutes public or private spaces becomes more complicated considering digital spaces. The Court examined this question in *Riley v. California*, where, after defendants were arrested and taken into police custody, law enforcement conducted searches of their cell phones and used information found therein to charge the defendants with additional offenses.[60] This case was a critical advancement in digital privacy, as there is a general tradition of allowing law enforcement to search the arrestee and the area around them in order to gather evidence incidental to the arrest.[61] The warrant exception in the "search incident to arrest" doctrine generally holds that once in police custody, the state has an interest in searching the area to preserve evidence required to assess and prosecute the crime, and the custodial and safety interests of law enforcement outweigh the arrestee's reduced (though not nonexistent) privacy interests once in custody.[62] In *Riley*, the court held that "police are generally required to obtain a warrant before searching digital information on an arrestee's cell phone."[63] This significant shift from previous permissible searching reflects the Court's understanding of the increasing pervasiveness of the information and digital footprint individuals carry in virtually universal technology (like a cell phone)—the kind of information that was unimaginable when earlier cases establishing the "incident to arrest" doctrine were decided.[64]

---

58. Hecht-Felella, *supra* note 4, at 5.

59. *Id.* at 6; Florida v. Riley, 488 U.S. 445, 450–52 (1989).

60. Riley v. California, 573 U.S. 373, 378–81 (2014).

61. *Id.* at 382–85.

62. *Id.* at 382–83, 391–92.

63. Hecht-Felella, *supra* note 4, at 6; *Riley*, 573 U.S. at 386.

64. *See Riley*, 573 U.S. at 386. Three major cases are credited with establishing the "incident to arrest doctrine." In *Chimel v. California*, the state overreached its arrest exception to a search warrant by searching the arrestee's entire home, including the garage and attic and even opening drawers. 395 U.S. 752, 754, 768 (1969). The Court held such a search was too extensive to be supported by the government's interest in preserving safety and evidence. *Id.* In *United States v. Robinson*, the officers completed a pat down search of the arrestee, finding heroin in a cigarette pack that fell out of his pocket, which the Court held within the "incident to arrest" exception because it was a "custodial arrest of a suspect based on probable cause . . . [and thus a] reasonable intrusion under the Fourth Amendment." 414 U.S. 218, 223, 235 (1973). Finally, in *Arizona v. Gant*, the Court held that police could be authorized to search the vehicle of an arrestee given the interests in officer safety and preservation of evidence inherent to the incident to arrest doctrine,

The Court reasoned that because cell phones are essentially ubiquitous aspects of daily life for adults and contain significant breadth and depth of personal information, and because the risks underlying the rationale of the search incident to arrest doctrine (officer safety and preservation of evidence) are not present with a digital search to the extent they were in the physical searches of arrestees, that "officers must generally secure a warrant before conducting such a search" of an arrestee's cell phone.[65]

The more technology continues to advance, the more complex questions become about the distinction between "public" and "private" places, as well as what could and should reasonably constitute a Fourth Amendment protected search for which a warrant is required. For example, in *Kyllo v. United States*, the Court expanded its understanding of technology and surveillance by holding that when the State uses technology that is not generally available and common in public use (in this case, thermal imaging technology to search the interior of a home) it qualifies as an unreasonable search and requires a warrant.[66] In this case, the Court weighed the differences between commonly available technologies related to public use, in contrast with more invasive technological capabilities that permit more invasive government action, with the hope that this would help future Courts keep up with technological baselines and allow the jurisprudence to evolve alongside technology.[67]

Finally, with its decision in *United States v. Jones*, the Court took major steps forward in considering the nexus of technological advancement; the idea of public and private spaces; and the amount of information gathered via a search that would cause any Fourth Amendment concerns.[68] In *Jones*, the Court determined that law enforcement's use of a GPS installed without a warrant on a suspect's vehicle and monitored for a month constituted a search under the Fourth Amendment and required a warrant.[69] This holding advanced *Katz* in a substantial way, as the Court considered the vehicle an "effect" under the Fourth Amendment, and in concurring opinions, several justices determined that using the GPS to obtain information about the suspect's movements over the duration of a month was too invasive to permit without requiring a warrant.[70] The

---

but qualified that the arrestee must be "unsecured and within reaching distance of the passenger compartment at the time of the search." 556 U.S. 332, 343, 350 (2009).

65. *Riley*, 573 U.S. at 387.

66. Hecht-Felella, *supra* note 4, at 6; Kyllo v. United States, 533 U.S. 27, 40 (2001).

67. Hecht-Felella, *supra* note 4, at 6.

68. *See* United States v. Jones, 565 U.S. 400 (2012).

69. *Id.* at 404.

70. *See* Hecht-Felella, *supra* note 4, at 6; *Jones*, 565 U.S. at 404–05. Justice Scalia wrote the majority opinion, and while the concurrences of other justices would have held that the information obtained by the GPS constituted such broad insight into the suspect's life that a warrant was required, Justice Scalia argued a narrower holding which was the official majority opinion. *Jones*, 565 U.S. at 413–14, 418 (Sotomayor, J., concurring); *id.* at 418–19 (Alito, J., concurring). His determination that the GPS monitoring required a warrant hinged on the idea that the *Katz* doctrine

technology used and the level of information gathered demonstrates a longstanding issue that the Court has wrestled with and one which Justice Sotomayor elaborated in her concurrence, namely that the third-party doctrine "is ill-suited for 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."[71]

3. Carpenter and its Updates

The most recent update to the Court's privacy jurisprudence was *Carpenter v. United States*. In *Carpenter*, the Court held that the government's accessing of location information from the defendant's cellular telephone service provider constituted a search.[72] The defendant, Timothy Carpenter, was prosecuted for his alleged involvement in a series of robberies.[73] The government sought access to cell-site location information (CSLI) from Carpenter's mobile service providers in order to corroborate allegations of his presence around the time of the robberies.[74] The government sought the CSLI under its authority granted under the Stored Communications Act of 1986, which permits the government to obtain disclosures of some telecommunication records so long as they show "reasonable grounds" that the information is "relevant and material to an ongoing criminal investigation."[75] The Stored Communications Act is one of the three legs of the broader federal Electronic Communications Privacy Act of 1986, passed with the intention to curb law enforcement's use of electronic communications data and to guarantee "Fourth Amendment like privacy protections."[76] As with the Fourth Amendment, law enforcement is able to overcome the privacy protections intended by the act if they meet the requisite standard, which was adequately applied in *Carpenter*'s circumstance.[77]

This is a major advancement in the understanding that some data is worthy of constitutional protection even when in the hands of third-parties and those

---

of a reasonable expectation of privacy in personal effects extended to a car and held that a car was an "effect" as established under the Fourth Amendment. *Id.* at 401, 404–05.

71. Hecht-Felella, *supra* note 4, at 7 (citing *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring)).

72. *Carpenter*, 585 U.S. at 313.

73. Hecht-Felella, *supra* note 4, at 8.

74. *Id.*; *Carpenter*, 585 U.S. at 301.

75. Hecht-Felella, *supra* note 4, at 8; Stored Communications Act of 1986, 18 U.S.C. § 2703(d).

76. MULLIGAN & LINEBAUGH, *supra* note 12, at 25.

77. In *Carpenter*, the Court did not hold that the access of the information violated the "reasonable grounds" and "relevant . . . to an ongoing criminal investigation" standard established in the SCA. *Carpenter*, 585 U.S. at 324–26; 18 U.S.C. § 2703(d). Rather, the Court held that the information and data obtained by that access—the CSLI used to map Carpenter's locations and movements over a period of days—was intrusive enough to reach the level requiring Fourth Amendment protections and would need a warrant and to follow proper procedure for searches. *See* Hecht-Felella, *supra* note 4, at 8.

parties follow the correct procedures around its access. *Carpenter* updated the third-party doctrine and necessitates consideration of additional factors in determining whether certain information falls within what would traditionally be considered private, and thus requires constitutional protections.[78] *Carpenter* also updated the Fourth Amendment jurisprudence covering digital privacy and added to the *Katz* interpretation that a digital search, not requiring a physical trespass, could still violate the protections in the Fourth Amendment.[79] Generally speaking, the factors the majority considered the most important in determining that the defendant was entitled to Fourth Amendment protections for his CSLI data were the data's "comprehensiveness, intimacy, expense, retrospectivity, and voluntariness."[80] These factors become more interesting when applied to the case of modern data brokers and the sale of individual consumer data.

The decision in *Carpenter* made two major advancements in the Fourth Amendment jurisprudence and understanding of the scope of Fourth Amendment privacy protections. First, the Court changed its interpretations of the kinds of technologies the Fourth Amendment is intended to protect against.[81] Instead of considering only newer, government-controlled technology not widely in public use, the Court extended the protection of the Fourth Amendment to technology in widespread, nearly ubiquitous daily use: the cell phone.[82] Second, the Court elaborated on the limitations of the third-party doctrine and considered that the extent of this doctrine is not well-equipped to address the continually evolving challenges of increasing technological intersections with American privacy concerns.[83]

a. Carpenter's Impact?

While the two changes in *Carpenter* establish important new foundations and backstops to the concerns facing individuals, there are still myriad unanswered questions and incremental changes that could leave many individuals vulnerable as courts continue to identify the Fourth Amendment's boundaries.

b. What Even Is My Data?

As a final note before analyzing the way *Carpenter* may update the Court's view of U.S. location data and the realm of data privacy generally, a brief survey of the technological aspects at play is warranted. The American public and legislators alike have viewed consumer data and the way it is protected as an

78. Hecht-Felella, *supra* note 4, at 9–10; *Carpenter*, 585 U.S. at 304–05.

79. *See* Hecht-Felella, *supra* note 4, at 8–9.

80. Hecht-Felella, *supra* note 4, at 8; *Carpenter*, 585 U.S. at 339–41 (Kennedy, J., dissenting) (highlighting the factors most important in the majority's opinion establishing their reasoning in holding for Carpenter).

81. Hecht-Felella, *supra* note 4, at 8; *Carpenter*, 585 U.S. at 304–09.

82. Hecht-Felella, *supra* note 4, at 8; *Carpenter*, 585 U.S. at 304–07, 311–314.

83. *See* Hecht-Felella, *supra* note 4, at 8; *Carpenter*, 585 U.S. at 309–10.

important topic for decades, demonstrated by the initial flurry of legislation aimed at protecting specific spheres of information.[84] The landscape of that data's usage has dramatically accelerated, with modern data brokers collecting, analyzing, generating, and selling user data profiles.[85]

Data brokers are "companies that collect consumers' personal information and resell or share that information with others."[86] The FTC considers data brokers within one of three general camps: "(1) entities subject to the FRCA; (2) entities that maintain data for marketing purposes; and (3) non-FRCA covered entities that maintain data for non-marketing purposes."[87] These companies gather information about users from a variety of sources, including "commercial, government, and other publicly available sources," and then assemble the disparate pieces of raw data into aggregated profiles about users, using both the raw information pulled from sources and the outputs of analysis data brokers perform using that raw information, rendering additional new, derived data about consumers.[88] While these services can often "help" consumers by allowing data brokers' clients to offer more personalized products to consumers, the amount of data they command is formidable and poses a serious privacy threat to individual users.[89]

The aggregation and additional information the data brokers gather creates extremely detailed pictures of an individual consumer's life, involving billions of data elements that cover nearly every consumer in the United States.[90] These companies then "combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences."[91] The complexities in these companies extend further, with data brokers supplying information to one another in building their data segments and consumer profiles, making tracing the origin of a specific consumer's data "virtually impossible" and "combin[ing] online and offline data to market to consumers online."[92] These profiles on consumers are sold as marketing tools to other companies, who use the information to target specific advertising campaigns to consumers they best

84. FED. TRADE COMM'N, *supra* note 50, at i. The initial driver behind the adoption of the Fair Credit Reporting Act, for example, was a concern about how data was used by companies without adequate transparency and communication to impacted consumers. The FCRA was passed in 1970. Fifty-three years later, the landscape is more intrusive and less protected.

85. *See* Robert Sheldon, *Definition: Data Broker (Information Broker)*, TECHTARGET, https://www.techtarget.com/whatis/definition/data-broker-information-broker [https://perma.cc/G225-59U8] (last visited Apr. 22, 2024).

86. *Id.*

87. FED. TRADE COMM'N, *supra* note 50, at i. Data brokers that fall outside the FCRA cover things like identifying fraud or location.

88. *Id.* at ii.

89. *Id.* at iv–vi.

90. *Id*. at iv.

91. *Id.*

92. *Id.* at iv–v.

align with.[93] In theory, that drives a more desirable product for the consumer, but there is virtually no regulation for how that information is used, leading to the potential for "facilitat[ion of] harassment, or even stalking, and may expose . . . individuals to retaliation or other harm."[94] Individuals have no insight into where their information originates, who houses it, how it is used, how to trace it, or how to potentially correct any erroneous information, and much of the collection and operations of these brokers occur without any awareness by the consumer at all.[95]

The other main avenue through which U.S. individual's data is gathered and used is by mobile apps on smartphones, including social media. Generally, smartphone users download apps on their phones for a wide variety of uses, and those apps gather information on the user ranging from "profile information such as age and gender to location details, including data about nearby cell phone towers or Wi-Fi routers, and information about every other app on a phone."[96] Much of that data is gathered by the parent tech company of either the phone or a broader application, but it is also traded to data brokers and among those networks. The change in the way apps have monetized their businesses, moving to primarily advertising, has led to a situation where "users, regulators and sometimes even the app developers and advertisers are unaware of the extent to which data flow from smartphones to digital advertising groups, data brokers and intermediaries that buy, sell and blend information."[97] Much of this data flows up to a higher tech umbrella or parent company, the most common being "Alphabet . . . Facebook, Twitter, Verizon, Microsoft, and Amazon."[98]

When this data similarly interacts with data brokers, additional information about users flows up, including location data and information with browsing in the app. The major difference between data brokers' gathering of information and that of mobile apps is the extent of control and awareness the user has of the information, with apps allowing individuals to opt out of some sharing and usage.[99] While that control is limited and requires significant understanding on the part of the user, it does offer a slightly different relationship between the user and the data gatherer, as compared with data brokers.

---

93. *See* Robert Sheldon, *supra* note 85.

94. FED. TRADE COMM'N, *supra* note 50, at i.

95. *See generally id.* at vi–vii. These data brokers collect personally identifying information from Internet users, including address, email address, purchase history, and other predictive information like buying habits and demographics. Data brokers then package, aggregate, and sell these packages of user information to other clients who use the information for primarily three uses: marketing, risk mitigation, and people search. *Id.*

96. Aliya Ram et al., *How Smartphone Apps Track Users and Share Data*, FIN. TIMES (Oct. 23, 2018), http://ig.ft.com/mobile-app-data-trackers/ [https://perma.cc/FDS5-T5RM].

97. *Id.*

98. *Id.*

99. *See A Day in the Life of Your Data*, APPLE 12 (Apr. 2021), apple.com/ca/privacy/docs/A_Day_in_the_Life_of_Your_Data.pdf [https://perma.cc/835S-U7AA].

II. ANALYSIS

The patchwork approach to U.S. data privacy legislation at both the state and federal levels inherently leaves gaps throughout the framework of protections, with intersecting pieces offering potential redundancies in some areas and major chasms of unprotected information in others. The existing interpretations of case law that trigger Fourth Amendment protections also leave unanswered questions about the kinds of data and information that are covered, the length of time encompassed by that data, and the threshold that constitutes a search. Additionally, questions of how previous doctrines continue to limit or expand the government's access to information remain open-ended. The legislation that is in place does not consider the types of businesses that market consumer data, or the social media applications that have such data and are willing to sell it.

The privacy implications of permitting governments and other state entities to purchase and access broad amalgamations of individual data pose a conundrum with facets that were inconceivable just decades ago. In the same vein, any proposed solution must explicitly consider the rapidity of developments in the technological landscape and consider the reality that any specific law regarding data today may be obsolete in a year and may fall laughably short of the future scope of the problem. Arguably, at the time of its passage in 1986, the ECPA was cutting edge technological protection and considered a groundbreaking advancement for the individual right to privacy in data and information. Less than forty years later, it is widely considered outdated in the current technological landscape. This is especially clear as background to the litigation in *Carpenter*, because in that case even though the government complied with the requirements of the ECPA's Stored Communications Act in their access of Carpenter's data, the Court still determined a Fourth Amendment search had occurred and a warrant was required.[100]

The current framework piecing together state and federal law along with Supreme Court precedent clearly leaves gaps in the fabric of U.S. privacy protections which stand to grow with the acceleration of technological advancements that make data brokers' and companies' practice of gathering, storing, and selling data easier and less expensive.

A. Statutory Gaps

1. State Gaps

States can seek to establish their own approach to the boundaries around appropriate usage of their citizen's information, but such boundaries can only apply to individuals within that state and cannot conflict with any superseding federal law. Even with such power, each state has approached protection of individual data differently, and, though varied, each approach is equally valid from a legal conflicts perspective. In other words, no state's approach to this

100. *Carpenter*, 585 U.S. at 316–18.

problem is by default legally granted more weight than any other. This can lead to challenges with individuals who travel between states for work or live in towns that straddle state borders. While only three states have now passed generally applicable statutory data protection, those laws only protect residents of those states or individuals within those states' borders at the time.

One such state, Virginia, offers an interesting example. If an individual lives in northern Virginia, works in the District of Columbia, and spends significant time in Maryland, the same person with the same cell phone is subject to three different state-level protection regimes for how his information is used, stored, accessed, and distributed. Commercial aggregation occurs constantly and in order for an individual to informedly adjust their behavior to protect their privacy from the sharing of cell phone information, one would potentially need to adjust their behavior multiple times over the course of a day. Clearly, this poses a substantial hurdle to the every day lives of many individuals, days that must now involve constant attempts to keep personal details safe. Additionally, it raises a question about the appropriate split between individuals, the companies that collect their data, those that store it, and those that disseminate it. If a telecommunications company has offices and services operating in one state, servers that hold aggregated data in another, and sales offices that distribute that information in still another, which state controls the use of the individual's information? Is it the state where the individual happens to be at the time? Or where the individual lives? Or where the different entities of the company operate, meaning all the data could be sent from Virginia to be stored in Maryland to avoid posing a problem? These questions can easily occupy full time employment for teams of compliance lawyers and conflict of laws professors. If the goal is information overload in the hopes that individuals give up on caring about how their data is used, when, and by whom, it seems to be on strong footing.

2. Federal Gaps

Any federal legislation would necessarily supersede state level legislation, but often tensions between the two create additional litigation. States will often allege that a certain federal action infringes on states' reserved general "police power." The first major issue with a fully legislative and statutory fix falls within the federalist structure of the United States. Because the federal government is one of limited powers, states retain substantial influence in their general police power and their ability to legislate over general matters relating to the individuals living within their borders. At the federal level, Congress can legislate with a relatively broad brushstroke, but still must remain within the enumerated Article I powers granted under the Constitution. This separation and split in the layers of American government has been the root of substantial Constitutional battles throughout the nation's history, and similarly leaves room for contention with respect to the application of data protections.

While Congress can provide for a federal right of action, it lacks the authority to establish how the Supreme Court should interpretat "searches" under the Fourth Amendment.[101] Though some federal legislation does exist, Congress's inability to dictate the Court's intrepration, and the capacity of any federal legislation to stay abreast of technological advances—such as the ways technology companies and data brokers generate, use, and sell user data—is seriously in doubt. No matter how generally written, well-intended, nor prescient, any new federal laws would be unlikely to address these problems. However, federal legislation can address the gaps that lawmakers see in the current protective scheme.

One aspect of legislative drafting is whether the law should be broad or narrow in scope. Narrow and precise legislation can give clarity to those seeking to comply with it, while overly narrow drafting will lead to potentially important things falling through the cracks. On the other hand, legislation that is too broad may create situations in which information is overly protected, so that people cannot communicate or share certain important information with individuals who have a genuine and non-nefarious interest in utilizing it. The tensions between drafting a statute narrowly enough to have meaningful impact and broad enough to have meaningful scope is a challenge.[102]

---

101. Even in circumstances of serious state disapproval of Supreme Court precedent and significantly supported legislation (such as the Religious Freedom Restoration Act (RFRA)of 1993), the Supreme Court still retains the power to determine the bounds and scope of the Constitutional rights allocated. *See* City of Boerne v. Flores, 521 U.S. 507, 519–20, 536 (1997) (overruling as unconstitutional RFRA and holding that while Congress has substantial legislative powers, they do not include the ability to dictate to the Court what its interpretation of the Constitution and its Amendments ought to entail, but do include the power to create a federal statutory cause of action for those who qualify). In a privacy case, Congress could similarly grant a federal right of action to individuals who have been harmed by what Congress determines is an improper use of their information and data. That will not amount to an interpretive framework for the Court in terms of where the bounds of a Fourth Amendment protected search begins and ends, but still would provide some form of recourse for individuals who suffer the kind of harm Congress deems impermissible in the realm of data privacy.

102. Some advocates of a standardized legislative answer consider the landmark European GDPR legal framework a solution the United States should use as a model. While the GDPR is a landmark set of regulations and requirements for privacy protections in Europe, and it includes compelling protections in the areas of disclosure by companies and the requirement for individuals to opt in and consent explicitly to certain uses of their information, there are challenges in using it as a template for a U.S. legislative scheme. The GDPR contains broader protections for data than proposed U.S. regulations, focusing on "any accumulation of data" as opposed to a sector-specific or industry specific approach common in the current U.S. scheme. MULLIGAN & LINEBAUGH, *supra* note 12, at 40. The legal requirements between different sovereign European nations in respecting the usage of data between and among those states poses a different standard of legal issue than what the internal governance of a country can do and how it can collect the information internally.

B. Gaps in Case Law and Litigation

1. Third-Party Doctrine Issues

Based on recent developments in third-party doctrine, there is no clear standard whereby an individual is protected from the warrantless review of information that the individual has directly or indirectly provided to a third-party. When there are services required for meaningful daily life (that is, Internet usage, cell phones, etc.) and those are the only providers of that service, can an individual reasonably be held to have voluntarily disclosed their information to them? For instance, Internet access is nearly universally acknowledged to be required for school and work. Can someone who is required to attend school, or who needs to work to support themselves reasonably be considered to have voluntarily shared information about themselves with a third-party?

2. Carpenter Issues: Scope, Time, and Data Type

Carpenter left many questions unresolved, including the applicability of its holding to any kind of data beyond CSLI, and any amount of time requested by law enforcement shorter or longer than seven days.[103] Questions about other data, the amount of time monitoring or searching will take, and at what point that time horizon crosses a constitutionally protected threshold persist, as well as the potential for the interaction of different kinds of information in the aggregate to create a broader informational picture that would require constitutional protection, while the individual's pieces of data that comprise that picture may not.[104] While the Court considered the "intimacy, comprehensiveness, expense, retrospectivity, and voluntariness" of the CSLI sought in *Carpenter*, there is no specific formula for how those factors apply outside the realm of CSLI.[105] For example, while the Court determined that the length of time used in the data gathered on *Carpenter* crossed over the threshold of comprehensiveness and retrospectivity at 127 days, it did not specify where that line is.[106] While 126 days could still be too invasive, what about 90? 60? Just a month, at 30 days? Similarly, the scope of information that spells "invasiveness" is unclear, leaving lines fuzzy. While location data clearly was deemed overly intimate, providing an extremely detailed picture of an individual's movements and habits, types of information that fall below that standard were not elaborated upon. Could social media application data, which

---

103. Hecht-Felella, *supra* note 4, at 8; *see Carpenter*, 585 U.S. at 314–16.

104. As with most judicial factors tests, the Court provided no guidance on the specific weight of each factor, posing challenges for those applying the test. States may try to enact their own legislation to see which laws push up to the edges and are overruled by the Court, but that strategy takes years, if not decades, and leaves substantial questions still unresolved.

105. *Carpenter*, 585 U.S. at 339–41 (Kennedy, J., dissenting) (highlighting the factors most important in the majority's opinion establishing their reasoning in holding for Carpenter).

106. *Id.* Of note, the Court seems to suggest that less than seven days of location information may not require a warrant. *Id.*

also collects location information, distinct from CSLI, trigger the same Fourth Amendment protection? Or is CSLI alone the kind of location information that is intimate and precise enough, and involuntary enough, to require constitutional safeguards?

Considering the voluntariness aspect of *Carpenter* as it melds with the problematic third-party doctrine, is there any reasonable way to interpret data as actually voluntarily disclosed to third parties today? Is it truly a "voluntary" disclosure when Google trends tracks someone's Internet usage, and then a data broker purchases and resells that information? As the concurrences and dissents demonstrated in *Carpenter*, the extent of the "voluntariness" of much of the information gathered about individuals seems to indicate that certain engagements are so ubiquitous in life that they cross from what can reasonably be considered as voluntary to something that is, in all practical senses, an involuntary aspect of living and productively engaging in modern society.

As Congress continues to wrestle with the issues inherent in any comprehensive scheme to regulate access to and use of information, and to protect privacy, it should consider how to address these problems via legislation. Such legislation should provide which information can and cannot be considered "voluntarily" disclosed to third-parties and should require that companies disclose to their consumers information like how and when their data is bundled, sold, and accessed.[107] This does not overstep the Fourth Amendment jurisprudence of the Court, and still allows the judiciary to function as intended, while giving federal legislators the impetus and incentive to begin to address the problem.

III. COMMENT

A. Dude, Now What?

Given the reality of the gaps between state and federal privacy law and the difficulties in posing solutions that do not jump ahead of Fourth Amendment jurisprudence, addressing the problem holistically is a complicated task. Like in bargaining approaches, the broader the solution, the more buy-in is possible to attain, while a narrower and more tailored approach may provide a more effective solution but alienate more individuals from buying into the solution collaboratively.

The most direct route to a successful scheme protecting the data privacy interests of U.S. citizens would be federal legislation. For the reasons discussed above, the current patchwork approach knitting together Supreme Court precedent, federal statutes of narrow purview, and state statutes, presents an inefficient and problematic strategy. While a comprehensive package is a desirable and worthwhile goal, Congress could focus on two specific areas to

107. *See* Comstock Ondrof, *supra* note 14, at 851; Goitein, *supra* note 14; Holland, *supra* note 14.

address the most urgent concerns while continuing to negotiate a broader package.

First, the legislature can address the issue of third-party disclosure once and for all. Though discussed in the *Smith* majority, the concurrences in *Jones*, and the dissents in *Carpenter*, the Court has never held that disclosure of information to a third-party is irrelevant to the degree of protection the data receives for Fourth Amendment purposes. The more interconnected our digital footprints are and become, the more information we inherently expose to third-parties. It is becoming increasingly unreasonable to believe that users intend to share the amount of information gathered about them with these parties. Even if that stretch is conceded, the subsequent sales of that information to advertising companies and groups that bundle, analyze, and resell the information are a step beyond the initial share. The conventional wisdom may argue that once disclosed, the information and the discloser has no further legitimate interest in the privacy of that information. Users would likely counter that, while they may have agreed to disclose certain information to platforms with the intention of being able to use the services and access the utilities provided by those applications and websites, they did not intend for their shared information to be continually sold, repackaged, and resold again, especially not to government purchasers who may then sidestep the usual Fourth Amendment requirements. The calculus of an individual's risk assessment when sharing information looks different if data is used by one application as required for the use of that specific service (like sharing location with a weather app to receive accurate localized weather updates), but that calculus likely changes when location information is shared with an infinite number of follow-on entities.

A legislative requirement that directly addresses the third-party disclosure component of privacy doctrine would offer one prong of relief and a welcome backstop as congressional leaders continue to work toward a comprehensive solution. Such a statute could hold that disclosure of the most intimate kinds of personal information cannot be considered a waiver of the individual's privacy interest in that information. This would offer a backstop to one major line of privacy policy analysis and more accurately reflects the realities of engaging with the digital world. A statute that refuses to allow the initial disclosure to third-party companies to be considered a "waiver" of the user's privacy interests would both acknowledge the virtually ubiquitous requirement to transmit otherwise private and intimate personal data to third-party companies in order to utilize services needed to engage with productive, daily American life and would offer an additional layer of protection by requiring the recipient company to take additional steps to access and use that information. An added benefit to this definitional aspect is its relative conceptual simplicity and common-sense appeal that makes it a potentially popular policy choice by leaders. This consensus policy would unite individuals from across the political spectrum behind the idea of protection of private, sensitive information.

The second aspect of an effective legislative approach would include more rigorous disclosure requirements by companies when user information is bundled, sold, or provided to additional parties. A massive concern in how data is utilized and sold is the murkiness and lack of transparency in how and where the information travels once it is transmitted to the first party beyond the original user. An additional requirement that when companies sell or further distribute information to downstream users after the primary disclosure from the original user, that the original user is notified of the details of the distribution, would promote transparency, and allow for stronger personal maintenance and awareness of the reach of a digital footprint. While being made aware of the sale of data or further disclosure would not change company disclosure policies and practices, it does give users more information and awareness of how they fit in the lifecycle of the data marketplace. While this would not grant any additional protections to users prior to their information being further distributed, it does shed light on the paths such information takes, provides users with appropriate notice, and gives more power to users to track the movements of that information.

These two aspects of a proposed legislative solution were included in the text of the proposed bipartisan Fourth Amendment Is Not For Sale Act.[108] While the bill had stalled in committee in the 117th Congress, there is hope that the more attention this issue gathers, especially in light of the many social issues it touches with regards to consumer data, the more likely that it will be reintroduced. While legislative capital is scarce, the more bipartisan support the proposal can gather, the stronger its chances of survival. Time is ticking, however, before campaign cycles resume and the issue is once again delayed until after the next election.

B. Criticisms

Critics of the proposed legislative policies could argue that the proposals are ineffective and not worth legislative capital since their impact may be negligible. Just because a company could no longer assume the waiver of an individual's privacy right when they disclose information to them that does not mean that company needs to change their policies in terms of advertising or future sales and use of data. The terms of service for all these companies easily could be updated to require affirmative explicit consent for that kind of use, and individuals can simply choose not to engage with them. Of course, the issue when this happens across the spectrum of digital platforms creates obstacles that seriously limit an individual's ability to engage meaningfully in society, but from the company side there could be potential pushback to the way they collect and use data and the consent of users to drive their business models with advertising.

Additionally, critics could argue that disclosure requirements would be too complex and not actually used by individual users. Most people do not read the

108. *See generally* S. 1265; H.R. 2738.

terms of service when they sign up for a new account on a website, and the idea that individuals will be invested enough to read every disclosure from a company to then make choices about how they engage with that company is arguably a stretch. It also might create a burdensome and overwhelming amount of information and disclosures, and companies could similarly flood individuals with information hoping to bury needles of potential problematic information uses in a haystack of disclosures such that people will lose interest and attention.

CONCLUSION

The "-isms" and "-ations" that define modern society are only increasing. The digitalization, globalization, capitalism, and innovation that define the American online experience is growing, becoming more interconnected, and blurring individual understanding as to where their information goes and who has access to it. The practice of companies aggregating and selling user information, often to government entities who purchase it to work around usage requirements that would typically necessitate a warrant, is sure to engender decresed confidence in the American government and to increased infringements of the privacy rights of many Americans. Incremental legislative changes that would change the definition of the "waiver" of a privacy expectation under the third-party doctrine and that would require disclosure to users when further distribution of their information occurs would offer greater transparency and ability for individuals to maintain awareness of their digital footprints. While comprehensive privacy protection may be far off and must be developed within the congressional legislative process, the perfect should not become the enemy of the good—smaller steps can offer immediate relief for individuals as the American digital privacy regime is developed and transitions into the future.