HARVARD LAW SCHOOL
NATIONAL SECURITY JOURNAL

ONLINE ARTICLE

Impractical and Unconstitutional: The Stored Communications Act Post-*Carpenter*

Richard McCutcheon[*1]

Recommended Citation

Richard McCutcheon, *Impractical and Unconstitutional: The Stored Communications Act Post-Carpenter*, HARV. NAT'L SEC. J. ONLINE (Oct. 17, 2024)

[*1] Assistant Attorney General for the State of Texas, Data Privacy and Security Enforcement Team, CIPP/US. B.A. University of Texas, 2018; J.D. The Ohio State University, 2021. The views expressed in this Article are those of the author and not presented as those of the Texas Attorney General's Office

Abstract

Perhaps no surveillance statute elicits more confusion and dismay in privacy professionals than the Stored Communications Act (SCA). As vague as it is labyrinthine, the SCA has created numerous interpretive issues and practical conundrums for judges and academics alike particularly in the context of internet surveillance. Originally conceived as a privacy-protective measure by Congress, the SCA has unintentionally provided law enforcement virtually unrestrained access to the inner lives of ordinary Americans and failed to keep pace with the advancement of technology. Despite the well-documented shortcomings of the SCA, reform efforts by Congress have been stymied.

With the Supreme Court's ruling in Carpenter v. United States, the SCA no longer is merely unintuitive and headache-inducing; it is unconstitutional. Carpenter opens the door to a litany of as-applied constitutional challenges to the SCA which, in essence, gut the entire act. This Article analyzes the implications of Carpenter on the SCA and suggests reforms to bring the SCA back within the realm of constitutionality.

TABLE OF CONTENTS

INTRODUCTION

The Stored Communications Act (SCA)[1] has generated numerous practical headaches for academics and judges as digital technology advances in scope and importance.[2] Created in 1986 as part of the Electronic Communications Privacy Act (ECPA), the SCA established the statutory regime that governs access to stored electronic communications by the government and third parties.[3] The SCA has been repeatedly criticized for being outdated and ill-suited for modern technology.[4] Despite a decade of continuous efforts to reform the SCA, none have been successful.[5]

Certain provisions of the SCA are not only unintuitive and confusing but unconstitutional as well.[6] The SCA empowers government entities to require digital service providers to disclose electronic communications stored in a system for 180 days or more by using a subpoena instead of a warrant.[7] The 180-day distinction is neither principled, nor constitutional.[8]

The constitutionality of the SCA's temporal subpoena authority has been primarily predicated on the Fourth Amendment's third-party doctrine.[9] The third-party doctrine states that individuals have a reduced privacy interest in records held by third parties, such as internet service providers.[10] Academics and commentators have strongly criticized the application of the third-party doctrine to digital technology.[11] Several states rejected the third-party doctrine by using the

---

[1] Stored Communications Act, 18 U.S.C. §§ 2701–2713.

[2] *See* Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTING L. J. 805, 820–21 (2003) (noting that electronic surveillance law is "famously complex, if not entirely impenetrable" and the difficulties federal judges have had with the SCA) [hereinafter Kerr, *Lifting the "Fog*"].

[3] *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208, 1214 (2004) [hereinafter Kerr, *A User's Guide*].

[4] *Id.*

[5] *See, e.g.*, Email Privacy Act, H.R. 1852, 113th Cong. (2013); Email Privacy Act, H.R. 699, 114th Cong. (2016); Email Privacy Act, H.R. 387, 115th Cong. (2017); Email Privacy Act, H.R. 8961, 116th Cong. (2020).

[6] *See* United States v. Warshak, 631 F.3d 266 (2010) (holding the SCA unconstitutional as applied to compelling production of emails without a warrant).

[7] 18 U.S.C. § 2703(a)–(b). Subpoenas may compel an individual or entity to testify, produce records, or appear for questioning provided the validity of the subpoena cannot be contested, whereas a warrant permits law enforcement to search and seize designated items subject to the warrant without prior notice—subpoenas are traditionally used to indicate a lesser level of protection and subject to a lesser legal standard than the probable cause required by warrants. *See, e.g.*, *In re 381 Search Warrants Directed to Facebook, Inc.*, 78 N.E.3d 141, 146–47 (N.Y. Ct. App. 2017),

[8] *See Warshak*, 631 F.3d at 288; Kerr, *A User's Guide*, *supra* note 3, at 1234; *see also* Timothy B. Lee, *Eric Holder Endorses Warrants for E-mail. It's About Time.,* WASH. POST (May 16, 2013, 4:46 PM), https://www.washingtonpost.com/news/wonk/wp/2013/05/16/eric-holder-endorses-warrants-for-e-mail-its-about-time/ [https://perma.cc/9FZT-M5SP] (quoting a Justice Department official opining that "'[t]here is no principled basis to treat e-mail less than 180 days old differently than e-mail more than 180 days old'").

[9] Kerr, *User's Guide*, *supra* note 3, at 1211–12.

[10] Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J. L. & TECH. 357, 362 (2019).

[11] *See, e.g.*, Daniel J. Solove, *Digital Dossiers and the Dissipation of Fourth Amendment Privacy*, 75 S. CAL. L. REV. 1083, 1136–38 (2002) (describing the shortcomings of the third-party doctrine); Jed Rubenfeld, *The End of Privacy*, 61 STAN. L. REV. 101, 113–14 (2008) (describing the third-party doctrine as the "Stranger Principle"). *But see* Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 561 (2009) (arguing for the retention of the third-party doctrine) [hereinafter Kerr, *The Case*].

Fourth Amendment equivalent found in their respective state constitutions.[12] The generally unfettered third-party doctrine allowed for the development of an immense and unprecedented surveillance state.[13]

Over the last decade, the Supreme Court has begun reconsidering the Fourth Amendment's third-party doctrine.[14] In *Carpenter v. United States*, the Court ruled that collection of cell-site location information (CSLI) under the SCA's subpoena authority was unconstitutional.[15] The Court justified its departure from the third-party doctrine by considering CSLI a special category of information worthy of full Fourth Amendment protections, requiring probable cause and a warrant to obtain.[16] Some commentators have speculated that *Carpenter* marked the end of the third-party doctrine as applied to digital data and have anticipated a massive overhaul to digital surveillance law.[17] Under the reasoning expressed in *Carpenter*, electronically stored communications should be considered information of a similar type to cell-site location information.[18]

In a post-*Carpenter* world, the 180-day clause of the SCA should be considered impractical at best and unconstitutional at worst for three reasons. First, constitutional and policy justifications for the SCA's regulatory scheme have always been ill-conceived for the information age. Second, *Carpenter* removes the critical constitutional justification of the SCA's temporal clause by effectively overturning the third-party doctrine *sub silentio*. Third, even if *Carpenter* did not abrogate the third-party doctrine, the Court in *Carpenter* strongly indicated that it would no longer apply the third-party doctrine to most electronic communications. In the wake of *Carpenter*, the SCA should be rewritten to be clearer and adhere to current Fourth Amendment jurisprudence.

I. THE WIRETAP ACT AND PAST JUSTIFICATIONS FOR THE SCA'S STATUTORY STRUCTURE

Initially conceived as a privacy protection regulation meant to address gaps in Fourth Amendment coverage,[19] the SCA today infringes on, rather than supplements, the Fourth

---

[12] Stephen Henderson, *Learning from All Fifty States: How to Apply the Fourth Amendment and Its State Analogs to Protect Third Party Information from Unreasonable Search*, 55 CATH. U. L. REV. 373, 395 (2006) (compiling state constitutional rulings).

[13] Margaret Hu, *Orwell's 1984 and a Fourth Amendment Cybersurveillance Nonintrusion Test*, 92 WASH. L. REV. 1819, 1821–22 (2017).

[14] *See, e.g.*, United States v. Jones, 565 U.S. 400, 417 (2012) (Sotomayor, J., concurring) (noting that the Court should reconsider the fundamental assumptions of the third-party doctrine); Carpenter v. United States, 138 S. Ct. 2206, 2209–10 (2018) (describing a lineage of cases where the Court has considered the third-party doctrine in the context of electronic surveillance).

[15] Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

[16] *Id.* at 2222.

[17] *See generally* Ohm, *supra* note 10, at 369–378 (describing a new three part "*Carpenter* test"); Michael Genthithes, *The End of Miller's Time: How Sensitivity Can Categorize Third-Party Data After Carpenter*, 53 GA. L. REV. 1039 (2019) (speculating that sensitivity of the information sought to be obtained will become a dominant factor and arguing for adjustments to the third-party doctrine); Matthew Tokson, *Inescapable Surveillance*, 106 CORNELL L. REV. 409 (2021) (considering inescapability the dominant factor for exceptions to the third-party doctrine); Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209 (2019) (anticipating a significant curbing of the third-party doctrine).

[18] *See Carpenter*, 138 S. Ct. at 2217–2219 (noting the importance of the type of data seized by the government).

[19] Kerr, *A User's Guide*, *supra* note 3, at 1210–11.

Amendment.[20] The 180-day storage clause of the SCA allows the government access to contents that would otherwise enjoy Fourth Amendment protection.[21] The disparate treatment of electronic communications based on a temporal distinction in the SCA has never been sufficiently justified by a policy or Fourth Amendment rationale.[22]

Since much of the statutory language and concepts incorporated in the SCA originate from the 1968 Wiretap Act,[23] a brief primer on the Wiretap Act is necessary. Each Act affords different levels of protection based on its own respective distinctions concerning the categories of information sought. In short, the Wiretap Act provides the intellectual baseline from which the SCA attempts to draw and distinguish itself. This outdated baseline has ultimately created problems for the SCA's application today.

In its most basic form, the Wiretap Act provides enhanced statutory protection, in addition to the Fourth Amendment's safeguards, for communications "intercept[ed]" using a surveillance device. [24] Essentially, the Wiretap Act not only prohibits the warrantless surveillance of communications while the communication is in transit, but also imposes additional statutory requirements for obtaining a warrant.[25]

Filling the holes not covered by the Wiretap Act, the SCA concerns "stored" communications held by "a provider of electronic communication service."[26] Under the SCA, a service provider may be subpoenaed to surrender electronic communications that have been stored in its system for more than 180 days.[27] In other words, the same communication which the Wiretap Act requires a specialized warrant to intercept in real time would be accessible by subpoena after a 180-day period.[28]

The distinctions in the statutes' treatment of intercepted and stored communications rest on three ill-formed justifications: (1) the third-party doctrine, (2) the concept of "abandonment" and (3) the retrospective-prospective surveillance distinction.[29] Each rationale fails to justify the overbearing reach of the SCA's subpoena authority and provides an outdated, impractical framework for addressing the competing interests of privacy and security in the modern

---

[20] *See, e.g.*, *Warshak*, 631 F.3d at 288 (holding unconstitutional the SCA's subpoena authority to obtain stored emails without a warrant).
[21] *See* 18 U.S.C. § 2703.
[22] *See* Lee, *supra* note 8.
[23] Omnibus Crime Control and Safe Streets Act, PUB. L. NO. 90-351, §§2510-2520, 82 Stat. 197, 211-25 (1968) (codified as amended at 18 U.S.C §§ 2510–2530 (2012)).
[24] 18 U.S.C. § 2511(1)(a) (2012).
[25] *See* 18 U.S.C. § 2518 (outlining the application procedure for intercepting communications).
[26] 18 U.S.C. 2703(a).
[27] *Id.*
[28] *Compare id.*, *with* 18 U.S.C. § 2511(1)(a).
[29] FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC SURVEILLANCE AND CIVIL LIBERTIES, 16, 40–42 (Office of Technology Assessment 1985) (explaining the state of Fourth Amendment jurisprudence and practical considerations for the distinctions in policy at the time of the enactment of the SCA); Kerr, *A User's Guide, supra* note 3 at 1209–12 (explaining how Fourth Amendment concepts informed the creation of the SCA); Orin S. Kerr, *Internet Surveillance Law After the USA Patriot Act: The Big Brother That Isn't,* 97 Nw. U. L. REV. 607, 616 (2003) (detailing the intellectual foundation of the distinction between retrospective and prospective surveillance) [hereinafter Kerr, *Internet Surveillance Law*].

technological landscape. The third-party doctrine and abandonment justifications both share an identical flaw of improperly analogizing distinctions conceived for physical property to digital data without considering the practical differences between the two. Likewise, the retrospective-prospective distinction creates a reductive hierarchy of data sensitivity based on temporal lines instead of taking into account the practical reality of how data is consumed and used. The intellectual framework from which the SCA emerged thus contains irreparable flaws that unjustifiably diminish American privacy.

A. The Third-Party Doctrine Justification: Broad, Impractical Nonsense

The third-party doctrine, a property-based distinction created by the Court's Fourth Amendment jurisprudence that empowers the government to seize property held by third parties without a warrant, has never worked in the context of digital data.[30] First established in *United States v. Miller*[31] and refined by *Smith v. Maryland*,[32] the third-party doctrine states that information voluntarily conveyed to a third party enjoys no expectation of privacy.[33] As the Court held in *Katz v. United States*, the Fourth Amendment does not protect against government searches when the individual has no reasonable expectation of privacy in the object of the search.[34] The logic underpinning the third-party doctrine comes from the assumption that the disclosing individual assumed the risk of the third party's disclosure of that information to the government, thereby extinguishing any expectation of privacy.[35] The third-party doctrine does not make any practical sense in the context of digital data, and the problems associated with it have contaminated the composition of the SCA.

While the third-party doctrine has roots specifically in the Fourth Amendment, the Court's logic extended beyond interpreting the Fourth Amendment into shaping the statutory schemes for surveillance regulations.[36] For instance, the Wiretap Act offers increased protections beyond the Fourth Amendment's warrant requirement and exclusionary remedies since citizens already have a Fourth Amendment protection from warrantless wiretaps.[37] By contrast, the SCA does little to supplement protection and offers no exclusionary remedy for its violation.[38] The lesser protections under the SCA mirror the perceived 'lesser' privacy interests in stored communications held by third parties under the Fourth Amendment.[39]

---

[30] *See Carpenter*, 138 S. Ct. at 2227 (Kennedy, J., dissenting) (explaining the origins of the third-party doctrine).
[31] 425 U.S. 435 (1976).
[32] 442 U.S. 735 (1979).
[33] *See id.* at 743–744 ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").
[34] 389 U.S. 347 (1967). *See also id.* at 360–61 (Harlan, J., concurring) (detailing what would become the Court's "reasonable expectation of privacy" test).
[35] *Smith*, 442 U.S. at 745.
[36] Kerr, *A User's Guide*, *supra* note 3, at 1209–11 (explaining the origins of the SCA).
[37] *See* Kerr, *Lifting the "Fog"*, *supra* note 2, at 814–15 (describing the "super warrant" necessary to obtain a court order under the Wiretap Act).
[38] *See* Kerr, *A User's Guide*, supra note 3, at 1243.
[39] *Id.* at 1209–11.

The SCA's statutory structure, when compared to the Wiretap Act, reflects the distinctions imposed by the third-party doctrine.[40] Communications in transit are not property held by any one individual given the nature of their constant movement.[41] Stored communications held by a third party, however, are the records of that third party.[42] According to the third-party doctrine, an individual has a lesser expectation of privacy in the records held by a third-party—a distinction not reflected by reality.[43]

The conceptual problems with the third-party doctrine in the context of digital surveillance have been extensively detailed by academics and privacy advocates.[44] The general expert consensus states that the third-party doctrine simply does not work as intended and greatly expands the government's surveillance capabilities without strong justification.[45] Since internet architecture requires the use of third parties to function, essentially all communications online are subject to the third-party doctrine.[46]

Online communications form the backbone of American social and financial lives in the twenty-first century.[47] People increasingly rely on the internet for everyday communication, dating, political participation, and financial services.[48] The categorical exclusion of information held by third parties from Fourth Amendment protection has given the government has access to people's most private information with a mere subpoena due to the SCA's limited statutory protection.[49]

The third-party doctrine creates a massive contradiction: despite the fact that many individuals' most private and intimate communications occur online, those communications have no reasonable expectation of privacy since the online technology requires third parties to function. Recognizing the issue, the Court has become more sensitive to the issues presented by the third-

---

[40] *See id.* at 1231.
[41] *See id.* (noting the practical differences in obtaining the information).
[42] *See id.*
[43] *See Carpenter*, 138 S. Ct. at 2235 (Thomas, J., dissenting) (noting the property-based distinctions that underpin the third-party doctrine). *See generally* Richard McCutcheon, Note, *Digital Data and the Fourth Amendment: The Bipartisan Solution*, 17 OHIO ST. TECH. L.J. 277, 283–300 (2021) (detailing the development of the property-based regime of the Fourth Amendment).
[44] Kerr, *The Case*, *supra* note 11, at 563 (noting that the third-party doctrine is the "rule scholars love to hate" and describing it as "the Lochner of search and seizure law").
[45] *See generally*, Neil Richards, *The Third-Party Doctrine and the Future of the Cloud*, 94 WASH. L. REV. 1441 (2017); Lucas Issacharoff & Kyle Wirshba, *Restoring Reason to the Third Party Doctrine*, 100 MINN. L. REV. 985 (2016); Bellovin et al., *It's Too Complicated: How the Internet Upends* Katz, Smith, *and Electronic Surveillance Law*, 30 HARV. J.L. & TECH 1 (2017).
[46] Solove, *supra* note 11, at 1089. *See also,* Bellovin et al., *supra* note 45, at 52–91 (describing in detail the complex structure of internet architecture).
[47] Paul Hitlin, *Internet, Social Media Use and Device Ownership in the U.S. Have Plateaued After Years of Growth*, PEW RSCH. CTR. (Sept. 28, 2018), https://www.pewresearch.org/fact-tank/2018/09/28/internet-social-media-use-and-device-ownership-in-u-s-have-plateaued-after-years-of-growth/ [https://perma.cc/XH7B-4LFM] (noting that use of digital technology has reached saturated levels high enough to prevent further growth).
[48] *See, e.g.*, SOCIAL MEDIA FACT SHEET, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/social-media/ [https://perma.cc/QNJ4-AJ8N] (noting 83% of American adults use at least one social media website).
[49] Joseph T. Thai, *Is Data Mining Ever a Search Under Justice Stevens's Fourth Amendment*, 74 FORDHAM L. REV. 1731, 1735 (2006) (noting that the Court "handed the government a blank check to conduct mass surveillance").

party doctrine in the last decade.[50] As discussed in Part III, the third-party doctrine has been increasingly questioned by the Court, and *Carpenter* may have put the final nail in the coffin.[51]

Even without the Court's recent reconsideration of the Fourth Amendment, the third-party doctrine as a policy decision makes little practical sense. Internet usage among Americans has become inseparable from everyday life, with essentially every American younger than age fifty utilizing internet services in some manner.[52] The recent COVID-19 crisis has only further highlighted the essential quality of internet to American life.[53]

The problems presented by the third-party doctrine are well-known and have only been exacerbated by technological development. As Professor Solove eloquently put it in his 2002 seminal work on the third-party doctrine from 2002, "[w]e are becoming a society of records, and these records are not held by us, but by third parties."[54] Today, individuals who want to participate in everyday society must surrender their information to third parties to use practically any digital platform.[55]

To permit the invasion of an individual's privacy as a cost for participation in society undermines the concept of a right to privacy itself. The SCA purports to be a privacy protection measure, but instead it allows almost limitless access to immensely sensitive information merely because those records are held by third parties. If an everyday person cannot hope to maintain privacy with regards to digital data, what privacy truly remains? If one's private sexual, political, personal, and emotional expressions can be readily obtained by the government without meaningful recourse to contest their collection, what can even be considered worth protecting?

Even in the days of *Smith* and *Miller*, the third-party doctrine was ill-suited to handle privacy issues.[56] As far back as the late 1970s when *Smith* was decided, service providers were already engaging in substantial data-collection practices beyond consumers' ability to control.[57] The problems inherent in the third-party doctrine have been exponentially magnified by the increasing importance of digital technology.

The untenable Fourth Amendment jurisprudence of the third-party doctrine infected the SCA at its inception. As a result, the SCA inherited an equally untenable, overly broad distinction in its statutory regime: the idea that digital records held by third parties warrant lesser protections.

---

[50] *See Jones*, 565 U.S. at 417 (Sotomayor, J., concurring); Riley v. California, 573 U.S. 373, 386, 392–398 (2014) (recognizing the need for increased protections for cell phones outside traditional Fourth Amendment jurisprudence).
[51] *See infra* Part III.
[52] *See Internet, Broadband Fact Sheet*, PEW RSCH. CTR. (Jan. 31, 2024), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/; *Mobile Fact Sheet*, PEW RSCH. CTR., (Jan. 31, 2024), https://www.pewinternet.org/factsheet/mobile/ [https://perma.cc/9P4J-SJWE].
[53] *See The Internet and the Pandemic*, PEW RSCH. CTR. (Sept. 1, 2021), https://www.pewresearch.org/internet/2021/09/01/the-internet-and-the-pandemic/ [https://perma.cc/W2CE-QRQL] ("90% of Americans say that the internet has been essential or important to them" during the COVID-19 pandemic).
[54] Solove, *supra* note 11, at 1089.
[55] Issacharoff & Wirshba, *supra* note 44, at 994–95.
[56] *See* Bellovin et al., *supra* note 45, at 4.
[57] *Id.*

The SCA's troubled upbringing created a Frankenstein's Monster of a surveillance law that achieves the opposite goals of its original intentions.

B. The Abandonment Justification: Should Be Abandoned in the Digital Sphere

The seemingly arbitrary decision to revoke protection for stored communications older than 180 days stems from a tortured application of the concept of abandonment.[58] For Fourth Amendment purposes, property is abandoned when a person can no longer claim a "continuing, legitimate expectation of privacy" concerning the property at issue.[59] While the test is fact dependent, the critical components of abandonment are actions indicating that the owner sought to relinquish ownership of the property.[60] Once the property has been abandoned, the property loses Fourth Amendment coverage.[61]

For physical property, the concept of abandonment makes intuitive, practical sense. After all, in most circumstances, when an individual has left physical property with a third party for an extended duration and made no effort to retrieve it, it is safe to assume that individual no longer cares about the property. For example, mail left unopened at the post office for over a year can be considered abandoned.[62]

The principles of abandonment cannot be easily applied to digital data. Unlike physical property, online data in the vast majority of circumstances cannot function independently or be withdrawn from the third-party service provider.[63] To use the mail example, it would be as if mail could only be viewed from the post office, and the post office retained its own copy of the mail. Even if one were to create one's own copy, the post office would still retain the mail. As a result, the third party always retains possession of the property in the digital sphere, unlike physical property. The amount of time data spends stored digitally does not reflect whether the end user intends to make use of it, and to use the data, the data inevitably must be stored with a third party.

Applying the concept of abandonment to digital data makes little sense and reflects the persistent problem of using pre-Internet jurisprudence in the context of digital data.[64] When the property in question always is held by the third party, there can be no meaningful expression of disowning based solely on the duration the third party held the property. Analogizing physical

[58] Kerr, *A User's Guide*, supra note 3, at 1234. Kerr speculates that the reason the concept was incorporated was due to a desire from the legislators to track with existing Supreme Court precedent of the time. *Id.*
[59] United States v. Robinson, 390 F.3d 853, 873 (6th Cir. 2004).
[60] *See* United States v. Jones, 707 F.2d 1169, 1172–73 (10th Cir. 1983).
[61] *Id.*
[62] *See Robinson*, 390 F.3d at 873. *Robinson* considered the seizure of a FedEx package sent to an expired mailbox and stored in the mailbox long after the package could have been disposed of by the post office. *Id.* at 874.
[63] *See* Bellovin, *supra* note 45, at 54–57 (describing how a variety of internet services require the use of third parties unknown to the end-user to function).
[64] *See* Kerr, *A User's Guide*, *supra* note 3, at 1234.

property concepts like abandonment to digital data ignores the substantial differences in how digital data operates.[65]

No compelling justification exists to incorporate the abandonment doctrine into the digital surveillance sphere. The Department of Justice itself admits the SCA's 180-day duration provides no principled rationale for its differential treatment and recommends removing it.[66] Abandonment has no place in justifying the SCA's subpoena authority.

C. The Retrospective-Prospective Distinction: The Distinction with No Difference

The third flawed reason for differential treatment between stored communication and communication in transit stems from a policy distinction in retrospective versus prospective surveillance.[67] Retrospective surveillance seeks to obtain information that already exists, whereas prospective surveillance obtains information as it is created.[68] Hence, "stored" communications being an important component of the SCA—and why "stored" information may be considered worthy of lesser protections when compared to the Wiretap Act, which seeks information in transit.

In the past, academics have viewed the privacy concerns implicated by retrospective surveillance as different from prospective surveillance, with the former implicating lesser privacy considerations than the latter.[69] The distinctions rest on considerations that lack merit in the modern technology-driven world.[70]

Given the scope and character of Americans' online interactions, the retrospective-prospective dichotomy can be considered a distinction without a difference. People place more information than ever before in the digital sphere, including their most intimate secrets and important information.[71] Stored communications often reveal people's political, sexual, religious, and familial associations.[72] That the information was obtained in real-time, rather than retroactively, does not change the sensitive nature of the information taken.

Academics have attempted to justify the retrospective-prospective distinction by illustrating two weak practical differences.[73] First, prospective surveillance can constitute a "dragnet" which inadvertently captures irrelevant or unneeded information for the government's

---

[65] *See id.* ("Incorporating [abandonment] principles into statutory law makes little sense. The SCA's drafters should have focused on finding the level of privacy protection that best balances privacy and security, not on finding the privacy protections that track Supreme Court cases decided long before the modern Internet."); Bellovin, *supra* note 45, at 54–57.

[66] U.S. DEP'T OF JUST., *Acting Assistant Attorney General Elana Tyrangial Testifies Before the U.S. House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations* (Mar. 19, 2013), https://www.justice.gov/opa/speech/acting-assistant-attorney-general-elana-tyrangiel-testifies-us-house-judiciary.

[67] Orin S. Kerr, *Internet Surveillance Law*, *supra* note 29 at 616.

[68] *Id.*

[69] *See id.* at 617.

[70] *See id.*at 616–18 (explaining the traditional rationales for creating lesser protections for retrospective surveillance).

[71] *See, e.g.*, *Jones*, 565 U.S. at 417 (Sotomayor, J., concurring).

[72] *Id.*

[73] *See, e.g.* Kerr, *Internet Surveillance Law*, *supra* note 29, at 616–618 (illustrating the practical differences between retrospective and prospective surveillance).

lawful objective.[74] By contrast, retrospective surveillance may be more limited by only capturing information that already exists and can be identified as proportional to the government's lawful objective.[75] Second, due to the aforementioned issues inherent to prospective surveillance, filtration remains a more challenging practical consideration for prospective surveillance and incidental observations of sensitive information may be more of a risk.[76]

Perhaps at one point where the subject matter and contents of stored digital information were limited in scope and importance, the retrospective-prospective justification had its place as a meaningful way to distinguish searches by sensitivity. However, in the modern age, where stored data contains extremely sensitive information regularly, the lesser status afforded to retrospectively obtained data does not make practical sense. Information obtained through each mode of surveillance can pry into private information.

Both retrospective and prospective surveillance present significant privacy concerns of the highest order. Even if prospective surveillance presents some additional privacy considerations, it does not justify the severely disparate treatment that the electronic surveillance statutory regime establishes between data in transit and stored data.

Further, the retrospective-prospective justification focuses on the wrong variable. Instead of concerning itself with what privacy interests are implicated, the retrospective-prospective distinction primarily considers the ease of filtration of information. Even if one disregards the filtration difficulties imposed by the vast amount of data searchable under the SCA, the focus on filtration subordinates a major privacy consideration to a minor enforcement consideration. The proper focus is on the sensitivity of the information captured, not the filtration of unnecessary or incidental information.

The retrospective-prospective distinction has become an outdated, meaningless distinction.[77] Prior to the modern information age, the distinction may have meant something practically, if still conceptually unprincipled, when the records held by third parties generally encompassed a limited species of data.[78] Considering the modern realities of how information is conveyed, however, the competing privacy interests in retrospective versus prospective surveillance are minimal. This flawed distinction created the backbone of SCA's statutory framework, distinguished it from the Wiretap Act, and contributed to its unworkable nature in the modern era.

---

[74] *Id.* at 616 (quoting Justice Douglas in *Berger v. New York*, 388 U.S. 41, 64–68 (1967) (Douglas, J., concurring)).
[75] *Id.*
[76] *Id.* at 617.
[77] The concept of information being "in transit" also presented interpretative difficulties for certain types of technologies and confused reviewing courts as to whether the Wiretap Act or the SCA was the applicable statute. *See* Kerr, *A User's Guide*, supra note 3, at 1232; United States v. Councilman, 373 F.3d 197, 203–04 (1st Cir. 2004) (holding emails copied in real time were "stored" and not "in transit").
[78] *See Carpenter*, 138 S. Ct. at 2218 (discussing how in the past, "attempts to reconstruct a person's movements were limited by a dearth of records").

II. *CARPENTER*: THE END OF THE THIRD-PARTY DOCTRINE AND THE SCA AS WE KNOW IT

The critical assumption forming the basis of the SCA's subpoena powers was that, due to the third-party doctrine, the Fourth Amendment did not protect stored communications.[79] Over the last decade, however, members of the Court have increasingly challenged the logic underpinning the third-party doctrine.[80] Those challenges, along with the Court's dissatisfaction with the third-party doctrine, culminated in the *Carpenter* decision and likely extinguished the doctrine entirely—despite the Court's protestation to the contrary.

A. Carpenter and Its Allegedly "Narrow" Holding

Carpenter concerned the FBI's search of cell-site location information ("CSLI") under the SCA.[81] Cell phones generate CSLI to connect to nearest "cell-site," which provides wireless service to the cell phone.[82] CSLI collects the phone's geographic location with a timestamp to assist in locating the nearest cell-site and performing a variety of other functions.[83]

The FBI sought 152 days of CSLI from MetroPCS and Sprint concerning Timothy Carpenter, a suspect in a string of armed robberies.[84] Using the SCA's subpoena powers, the FBI obtained the information, and Carpenter was convicted at trial.[85] Carpenter appealed his conviction on the grounds the CSLI had been obtained without a warrant in violation of the Fourth Amendment.[86]

The Court agreed with Carpenter that a warrant was required for the government to obtain the CSLI data for use against him at his trial.[87] In a 5-4 decision, the Court determined that due to the revealing and automatic nature of CSLI, the acquisition of the data was a search under the Fourth Amendment.[88] Writing for the majority, Chief Justice Roberts noted the decision was "narrow" and not intended to disturb the ordinary application of the third-party doctrine.[89] Nonetheless, the principles expressed in *Carpenter* reveal that the decision may not be as narrow as Chief Justice Roberts stated.[90]

---

[79] *See* Kerr, *A User's Guide,* supra note 3, at 1210–12; William Jeremy Robison, Note, *Free At What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L. J. 1195, 1226–27 (2010).
[80] *See generally Jones*, 565 U.S. 400 (holding warrantless vehicle tracking unconstitutional); *Riley*, 573 U.S. 373 (holding warrantless search and seizure of a cellphone incident to an arrest as unconstitutional); *Carpenter*, 138 S. Ct. 2206 (holding warrantless search and seizure of cell site location information unconstitutional).
[81] *Carpenter*, 138 S. Ct. at 2212.
[82] *Id.* at 2211.
[83] *Id.* at 2212.
[84] *Id.*
[85] *Id.* at 2213.
[86] *Id.*
[87] *Id.* at 2223.
[88] *Id.*
[89] *Id.* at 2220.
[90] Trevor Burrus & James Knight, Katz *Nipped and* Katz *Cradled:* Carpenter *and the Evolving Fourth Amendment*, 2018 CATO SUP. CT. REV. 79, 80 (2018).

The dissenting members of the Court expressed significant doubts that the holding of *Carpenter* could be constrained to the "narrow" facts presented in the case. In his dissent, Justice Gorsuch remarks that *Carpenter* put the third-party doctrine on "life support."[91] Former Justice Kennedy, in his dissent joined by Justices Thomas and Alito, expressed a similar skepticism about the narrowness of the Court's holding, predicting "dramatic consequences."[92] The dissenting Justices' skepticism is warranted. Since the SCA relies on the third-party doctrine to empower its subpoena authority, the Court's questioning of the third-party doctrine's legitimacy threatens the legitimacy of the SCA's subpoena authority by extension.[93]

B. Carpenter's Holding: Anything But "Narrow"

The logic forming the holding of *Carpenter* cannot be contained to the specific facts presented in the case. Chief Justice Roberts noted that the third-party doctrine fails to "contend with the seismic shifts in digital technology . . . . [and the] world of difference between the limited types of personal information addressed in *Smith* and *Miller* [compared to CSLI] . . . ."[94] In responding to Justice Kennedy's dissent, Chief Justice Roberts considered Justice Kennedy's proposed exception to third-party doctrine for the "modern-day equivalent of an individual's own 'papers' or 'effects'" to be "sensible".[95] Such an exception would already radically alter the scope of the third-party doctrine—and the SCA—by extending categorical protection from warrantless search to most electronic communications. Chief Justice Roberts did not stop here to conclude the case with only Justice Kennedy's proposed rule.

Instead, Chief Justice Roberts went even further, suggesting that specific types of non-content data are categorically excluded from the normal operation of the third-party doctrine. Comparing the seized data at issue, Chief Justice Roberts highlighted a contrast between the "exhaustive chronicle" of information at issue held by modern wireless carriers and the "limited capabilities" of the information obtained in *Smith*.[96] In addition, Chief Justice Roberts disputed that the information can be voluntarily shared, as characterized in *Miller*.[97] Consequently, data concerning pervasive and intimate parts of daily life similar to CSLI would be insulated from the third-party doctrine.

Limiting the application of *Smith* and *Miller* calls into question the basic precepts upon which the third-party doctrine is founded. Namely, the Court redirected the inquiry from who possesses the information to the nature of the information sought and how it was collected. Whether the information is held by a third party no longer dominates the analysis. Instead, the nature of the data sought guided the Court's intuitions as to what should be protected and what should not, with the involvement of third parties being a secondary, but not always relevant consideration. By altering the focus of the analysis away from the holder of the data and to the

---

[91] *Carpenter*, 138 S. Ct. at 2272 (Gorsuch, J., dissenting).
[92] *Id.* at 2233 (Kennedy, J., dissenting).
[93] While concepts like abandonment and the retrospective-prospective surveillance distinction have provided justifications for the existence of the SCA's statutory regime, neither justification has been held sufficient for empowering the SCA's subpoena authority absent the existence of the third-party doctrine.
[94] *Id.* at 2219.
[95] *Id.* at 2223 (citing *id.* at 2230 (Kennedy, J., dissenting).
[96] *Id.* at 2219.
[97] *Id.* at 2220.

sensitivity of the data, the Court abandoned the core of the third-party doctrine, leaving a hollow facsimile of this infamously broad categorical exception.

Carpenter likely ended the third-party doctrine, and by extension, the SCA's 180-day subpoena powers. Without explicitly saying so, the Court pulled the rug out from the SCA by vastly reducing the scope of the third-party doctrine to such a degree that it effectively no longer exists. As a result, the SCA's subpoena powers cannot be constitutional since the underlying constitutional justification dissipated. Post-*Carpenter*, stored communications enjoy full Fourth Amendment protections regardless of duration stored and cannot be obtained through subpoena.

III. *CARPENTER* AND *WARSHAK*: READING THE COURT'S TEA LEAVES

Even if the third-party doctrine has not been overturned, *Carpenter* still renders the SCA's temporal clause unconstitutional. Reading between the lines in both the *Carpenter* opinion and the dissents reveals that the Court almost certainly adopted the holding of *Warshak v. United States*[98] from the Sixth Circuit without explicitly saying so.[99] By adopting *Warshak*, the Court effectively abrogated the SCA's temporal clause.

A. The Warshak Rule and Carpenter

The Court's silent adoption of *Warshak* confirms the Court's intent to upend the foundation empowering the SCA's subpoena authority and limit its scope. *Warshak* concerned an application of the SCA's subpoena powers to obtain e-mails.[100] As part of a major fraud investigation, the government seized 27,000 of Steven Warshak's emails from his internet service providers using the SCA's subpoena powers.[101] The Sixth Circuit ruled the third-party doctrine could not be applied to e-mails any more than it could be applied to physical mail, and the SCA as applied was unconstitutional.[102] After *Warshak* was decided, the United States declined to appeal the issue further because the information it sought still could be obtained under the good faith exception.[103]

Due to the United States' decision to not appeal, the *Warshak* rule remained limited to the Sixth Circuit. Legislators attempted several times to give *Warshak*'s holding a nationwide reach through the numerous iterations of the Email Privacy Act, but despite bipartisan support, the bill never passed both the House and Senate.[104] Apparently taking notice of the issue, the Court in *Carpenter* implicitly adopted the central holding of *Warshak*.

---

[98] 631 F.3d 266 (6th Cir. 2010).
[99] *See Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting) (citing *Warshak*, 631 F.3d at 283–88); *id.* at 2269 (Gorsuch, J., dissenting) (citing *Warshak*, 631 F.3d at 285–86).
[100] *Warshak*, 631 F.3d at 282.
[101] *Id.*
[102] *Id.* at 288.
[103] *Id.* at 282.
[104] *See, e.g.*, Email Privacy Act, H.R. 1852, 113th Cong. (2013); Email Privacy Act, H.R. 699, 114th Cong. (2016); Email Privacy Act, H.R. 387, 115th Cong. (2017); Email Privacy Act, H.R. 8961, 116th Cong. (2020); *see also* Sophia

True, the majority opinion never expressly says the Court intends to adopt *Warshak*, but the contextual use of *Warshak* within the opinion makes clear the Court's intentions. All nine Justices of the 2018 Court agreed with the *Warshak* rule.[105] The majority opinion and the two dissents[106] in *Carpenter* favorably cite *Warshak*.[107] Taken together, every Justice on the Court in 2018 joined at least one opinion that discussed *Warshak* favorably.[108]

B. The Majority and Justice Kennedy's Use of Warshak

Admittedly, the majority employed a convoluted mechanism of adopting the *Warshak* rule. Chief Justice Roberts favorably cites to Justice Kennedy's dissent, which in turn cites to *Warshak.*[109] In essence, Justice Kennedy notes that the third-party doctrine does not apply when the government seeks to obtain information that is the modern-day equivalent of an individual's papers and effects.[110] In Justice Kennedy's dissent, a citation to *Warshak* follows the rule statement, noting in the parenthetical that "e-mails held by Internet service providers" as information protected by the Fourth Amendment.[111]

Writing for the majority, Chief Justice Roberts in turn cites Justice Kennedy's rule statement from *Warshak*, describing it as a "sensible exception."[112] Chief Justice Roberts goes on to state that the clear implication from Justice Kennedy's rule statement is that "documents," meaning e-mail and other "modern-day equivalents of … 'papers' or 'effects,'" should enjoy Fourth Amendment protection.[113] Summarizing the disagreement between the majority and Justice Kennedy, Chief Justice Roberts follows by stating that the Fourth Amendment protection "should extend *as well*" to CSLI.[114]

That "as well" provides unambiguous indication that the Court agreed with Justice Kennedy's adoption of *Warshak*. Because the root of the disagreement between Justice Kennedy and the majority stems from the inclusion of CSLI — not the use of *Warshak* — the Court and

---

Cope, *House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform*, ELECTRONIC FRONTIER FOUNDATION (Apr. 27, 2016), https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform (noting that the Email Privacy Act codifies the holding in *Warshak*).

[105] *See Carpenter*, 138 S. Ct. at 2222 (citing *Warshak*, 631 F.3d at 283–88); *id.* at 2230 (Kennedy, J., dissenting) (citing *Warshak*, 631 F.3d at 283–88); *id.* at 2269 (Gorsuch, J., dissenting) (citing *Warshak*, 631 F.3d at 285–86).

[106] *Carpenter* contained four dissents: Kennedy, Thomas, Alito, and Gorsuch. *See Carpenter*, 138 S. Ct. at 2211. Thomas and Alito's dissents do not mention *Warshak*. *Id.* at 2235–46 (Thomas, J., dissenting); *Id.* at 2246–61 (Alito, J., dissenting).

[107] *See Carpenter*, 138 S. Ct. at 2222 (citing Justice Kennedy's dissent, which cites *Warshak*); *id*. at 2230 (Kennedy, J., dissenting) (citing *Warshak*, 631 F.3d at 283–88); *id.* at 2269 (Gorsuch, J., dissenting) (citing *Warshak*, 631 F.3d at 285–86).

[108] *See Carpenter*, 138 S. Ct. at 2211. Justices Roberts, Ginsburg, Sotomayor, Kagan, and Breyer joined the majority. *Id.* Justices Alito and Thomas joined Kennedy's dissenting opinion. *Id.* at 2223 (Kennedy, J., dissenting). Justice Gorsuch wrote a solo dissent not joined by the other dissenters. *Id.* at 2261 (Gorsuch, J., dissenting).

[109] *Id.* at 2222 (citing *Carpenter*, 138 S. Ct. at 2230 (Kennedy, J., dissenting)).

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

[111] *Id.*

[112] *Id.* at 2222 (citing to *Carpenter*, 138 St. Ct. at 2230 (Kennedy, J., dissenting)).

[113] *Id.*

[114] *Id.* (emphasis added).

Justice Kennedy can fairly be said to agree on *Warshak*, and thus, *Warshak's* rule can be considered effectively part of the holding in *Carpenter*.

C. Justice Gorsuch's Use of Warshak

By contrast, Justice Gorsuch did not mince words when invoking Justice Kennedy's use of *Warshak*. Justice Gorsuch remarks that "few doubt that e-mail should be treated much like the traditional mail it has largely supplanted."[115] The phrasing reveals the apparent consensus the Court reached: the *Warshak* rule should be adopted.

Justice Gorsuch explicitly signposts his approval of *Warshak* by tying it to his bailment analysis, which is mentioned throughout the opinion.[116] The core of Justice Gorsuch's analysis relies on the fact that digital data can be protected under the common law concept of bailment.[117] As a result, by considering e-mail a form of bailment, Justice Gorsuch adopts the central holding of *Warshak*.

D. Why the Invocation of Warshak Matters

Adopting *Warshak* would substantially shrink the amount of content accessible under the SCA's grant of subpoena powers. The principles of *Warshak* can be easily transposed to other types of digital data.[118] Electronic communications such as e-mail, instant/private messaging, snapchats, browsing history, and other sensitive data will no longer be accessible under the SCA.[119]

The SCA's subpoena powers are vulnerable to a litany of as-applied constitutional challenges. Since the definition of "electronic communication" under the SCA carries a broad meaning which includes non-sensitive, non-communicative content like certain types of metadata, the SCA could still withstand a facial constitutional challenge.[120] Nonetheless, given

---

[115] *Id.* at 2269 (citing to *Carpenter*, 138 St. Ct. at 2230 (Kennedy, J., dissenting)).
[116] *See id.*
[117] *See id.* ("Whatever may be left of Smith and Miller, few doubt that e-mail should be treated much like the traditional mail it has largely supplanted—as a bailment in which the owner retains a vital and protected legal interest.").
[118] *Carpenter* in general has triggered an avalanche of academic papers speculating on the various technologies now covered under the Fourth Amendment. *See generally* Sarah Murphy, Note, *Watt Now?: Smart Meter Data Post-*Carpenter, 61 B.C. L. REV. 785 (2020) (discussing smart meter data); Paul Belonick, *Transparency Is the New Privacy: Blockchain's Challenge for the Fourth Amendment*, 23 STAN. TECH. L. REV. 114 (2020) (discussing cryptographs); Johanna Sanchez, *A New Era: Digital Curtilage and Alex-Enabled Smart Home Devices,* 36 TOURO L. REV. 663 (2020) (discussing the smart home).
[119] *See* Belonick, *supra* note 118, at 157 (suggesting that *Carpenter* "shared" by the necessities of modern life will forestall the third-party doctrine).
[120] *See* 18 U.S.C. § 2510(12) (1986) (defining "electronic communication" as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic or photooptical system that affects interstate or foreign commerce"). A facial constitutional challenge requires that every application of the law contain a defect that renders it unconstitutional, whereas an as-applied constitutional challenge requires only the statute to be unconstitutional as applied to the specific facts of the case. *See* MDK, Inc. v. Village of Grafton, 345 F. Supp. 2d 952, 959 n.10 (E.D. Wis. 2004).

the numerous and growing methods of internet communication, the SCA's broad subpoena grant will be chipped away in the coming years as more constitutional challenges emerge.

IV. AMENDING THE SCA

For decades, privacy advocates attempted to amend the SCA without success.[121] Now that the constitutional framework underlying the SCA has become virtually untenable, the need to amend the SCA has become even more pressing.[122] Post-*Carpenter*, the courts have been swamped by a menagerie of as-applied challenges to the SCA, and *Carpenter* itself does not provide exact guidance to lower courts on how to apply its rule.[123] Instead of subjecting the SCA to an innumerable number of as-applied constitutional challenges for every new technology under the sun, Congress should take the initiative and reform the SCA.

A. Removing the 180-Day Subpoena Power

At minimum, Congress needs to rethink the 180-day subpoena clause. The distinctions contained in the 180-day provision simply do not hold water and never did.[124] The clause as written grants access to a wide variety of data that is actually protected by the Fourth Amendment.[125] If data enjoys Fourth Amendment protections, it will not be accessible with a subpoena regardless of whether it was stored for 180 days. In essence, the "stored" part of the SCA needs to be removed.

If Congress wants to retain a limited subpoena authority in the SCA, it should target certain types of non-sensitive, non-content data,[126] such as third-party records of metadata, instead of relying on a duration-based distinction. Non-sensitive data could include internet protocol addresses, transactional metadata, data displayed publicly, reference metadata, etc.[127] By removing the time limit and instead identifying specific kinds of data accessible through subpoena, Congress can provide greater clarity and avoid infringing on the Fourth Amendment.

---

[121] *See, e.g.,* Email Privacy Act, H.R. 1852, 113th Cong. (2013); Email Privacy Act, H.R. 699, 114th Cong. (2016); Email Privacy Act, H.R. 387, 115th Cong. (2017); Email Privacy Act, H.R. 8961, 116th Cong. (2020).
[122] *See supra* Parts II–IV.
[123] *See* Tokson, *supra* note 17, at 412–14.
[124] *See* Kerr, *A User's Guide*, *supra* note 3, at 1234 ("Incorporating those weak Fourth Amendment principles into statutory law makes little sense. The SCA's drafters should have focused on finding the level of privacy protection that best balances privacy and security, not on finding the privacy protections that track Supreme Court cases decided long before the modern Internet."). Kerr's article was written in 2004. The idea that the temporal subpoena authority of the SCA was unconstitutional pre-*Carpenter* had been suggested by student authors over a decade ago. *See* Alexander Scolnik, Note, *Protection for Elections Communications*: *The Stored Communications Act and The Fourth Amendment*, 78 FORDHAM L. REV. 349, 351 (2009).
[125] *See Carpenter*, 138 S. Ct. at 2223; *Warshak*, 631 F.3d at 285–86.
[126] There is substantial indication that the traditional content/non-content distinction creates additional Fourth Amendment problems in digital contexts. *See* Matthew J. Tokson, *The Content/Envelope Distinction in Internet Law*, 50 WM. & MARY L. REV. 2105, 2124–25 (2009); Bellovin, *supra* note 45, at 19. Since the distinction applies to other surveillance statutes beyond the Stored Communication Act, such as the Wiretap Act and Pen Register Act, a protracted discussion of the merits of the content/non-content distinction is outside the scope of this article.
[127] For a detailed discussion on evaluating the sensitivity of various types of data, see Genthithes, *supra* note 17, at 1069–71.

Limiting the subpoena authority to a specific set of known technology anticipates the growing pains associated with essentially all technology-related laws.[128] When a statute provides broad authorities to large swathes of potential technology, as the SCA did, the broad application inevitably has unexpected and deleterious consequences. By contrast, limiting the language of the subpoena authority to known technology prevents the statute from operating in unpredictable ways. Rather than grant broad subpoena powers through the SCA, Congress should only include species of data known to withstand Fourth Amendment scrutiny.

Refining the statutory framework carries practical benefits as well. Adjusting the SCA's statutory protections to reflect the current scope of the Fourth Amendment and to provide clearly enumerated rights will save the judiciary the expenses and headache of sorting through the many as-applied challenges arising out of *Carpenter*. Further, clear statutory language can supply direct guidance to lower courts in a way that an articulation of constitutional principles cannot.

Such reforms would achieve at least three important ends. First, circumscribing the scope of the SCA would protect members of the public from unwarranted intrusion into their privacy. Second, greater clarity would prevent the law from operating in ways contrary to Congress' intention due to unanticipated technological developments.[129] Finally, achieving greater predictability from the legal system would allow for more equitable enforcement of the right to privacy by reducing arbitrary decision-making across all federal jurisdictions and clarify the responsibilities of private actors hosting data.[130]

B. Looking Forward: Taking Inspiration from European Statutory Law

Congress can look to the European Union's General Data Protection Regulation (GDPR)[131] for guidance on how to make the SCA more robust. The GDPR protects consumers by granting them limited ownership and rights to digital data held by third parties.[132] These rights include the right to access certain information stored by third parties, the right to delete certain data, and the right to object to the collection of certain data.[133] The GDPR's ownership rights reflect a modern understanding of the relationship individuals have with their data and allows individuals greater autonomy over their data.

---

[128] *See* Bellovin, *supra* note 45, at 92, 98–99 (noting the difficulties in adapting outdated technology laws through analogy).
[129] *See* Daniel Solove, *Further Thoughts on ADPPA, the Federal Comprehensive Privacy Bill*, TEACHPRIVACY (Jul. 30, 2022), https://teachprivacy.com/further-thoughts-on-adppa-the-federal-comprehensive-privacy-bill/ (explaining the necessity of "dynamism" in technology legislation).
[130] *See Letter to Chairman Pallone and Ranking Member McMorris Rodgers,* BUSINESS ROUNDTABLE 1–2 (Sept. 30, 2022), https://s3.amazonaws.com/brt.org/Business-RoundtableCommentsontheAmericanDataPrivacyandProtectionAct9.30.22.pdf [https://perma.cc/JQH9-D7H7] (expressing support for a comprehensive privacy framework to create greater clarity and guidance in American law).
[131] Commission Regulation 2016/679, 2016 O.J. (L 119). The GDPR provides several restrictions on the handling of data transferred between public and private entities, as well as violations for noncompliance. *See id.*
[132] *See generally* Jacob M. Victor, Comment, *The EU General Data Protection Regulation: Toward a Property Regime for Protecting Data Privacy*, 123 YALE L.J. 513 (2013).
[133] Council Regulation 2016/679, *supra* note 131, at ch. 3.

If the SCA granted a quasi-property interest in stored information similar to the GDPR, it would better serve its intended purpose of protecting data privacy. Under the SCA, end users have no ability or authority to restrict digital service provider collection of their data, allowing digital service providers to retain staggering amounts of end user data. Permitting end users to request and access the data stored by digital service providers creates a greater sense of transparency on what data these entities possess. Transparency gives end users the knowledge they need to make informed decision on how to tailor their online presence through exercising a right to delete or refusal to enable data collection. Allowing end users to delete and restrict the collection of data by digital service providers will also reduce the amount of data accessible by government entities.

By adopting the principles of the GDPR, Congress can achieve the SCA's intended purpose and enhance privacy rights rather than undermine them. The GDPR's limited property structure mirrors the concepts advocated for by the Court in *Carpenter* and in Justice Gorsuch's dissent.[134] Allowing for a limited property framework like the GDPR's minimizes the "all or nothing" problems created by the third-party doctrine and its progeny, furthering greater recognition of end user property rights.[135]

C. Potential Developments in American Privacy Legislation: The American Data Privacy and Protection Act and the American Privacy Rights Act

Introduced on June 21, 2022, the American Data Protection Act ("ADPPA") represented an important step forward in creating a comprehensive federal privacy regime similar to the GDPR.[136] The Act would have established consumer data protections and data handling policies, limited the collection of certain species of data, and granted a right to delete data, among other significant reforms.[137] While the ADPPA did not cover federal entities and a detailed assessment of its merits are not the objective of this Article, the greater attention to privacy-related issues indicates that SCA reform may be on the horizon. Unfortunately, despite nearly unanimous support from Democrats and Republicans in the House Energy & Commerce Committee, the Act faced significant difficulties to becoming law and ultimately did not pass.[138]

Even though reform was closer than "we have ever been," the ADPPA did not become law because of the wedge issue of state law preemption.[139] Specifically, the ADPPA would have preempted the stronger existing state law in California, which proved to be divisive for House

---

[134] *Carpenter*, 138 S. Ct. at 2219–20 (noting that the court must take into account the more sophisticated development of technology and recognizing CSLI as a distinct category of information); *id.* at 2270 (Gorsuch, J., dissenting) (arguing for quasi-property rights for digital data in the form of bailment).

[135] *See Smith*, 442 U.S. at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes.").

[136] American Data Privacy and Protection Act, H.R. 8152, 117th Cong. (2022).

[137] *Id.*

[138] *The American Data Privacy and Protection Act*, ABA (Aug. 30, 2022), https://www.americanbar.org/advocacy/governmental_legislative_work/publications/washingtonletter/august-22-wl/data-privacy-0822wl/.

[139] Allison Schiff, *Is There Still Hope for a Federal Privacy Bill This Year?* ADEXCHANGER (Sept. 7, 2022 10:50 AM), https://www.adexchanger.com/privacy/is-there-still-hope-for-a-federal-privacy-bill-this-year/ (quoting Caitlin Fennessy, Vice President and Chief Knowledge Officer of the International Association of Privacy Professionals).

Democrats and ultimately caused the bill to stall out without passage.[140] Although the desire for reform still exists, the future of the ADPPA's ideals remains uncertain.[141]

Industry experts and privacy professionals suspected that if ADPPA was not passed while the energy for reform existed, the opportunity for reform would be lost.[142] If a compromise on the preemption issue could revive ADPPA, Congress would be wise to take it. Congressional inaction in the privacy space cannot continue, and the American people cannot coast by on a patchwork of industry-specific regulations and federal legislation from before the invention of the smartphone.

Unfortunately, reform still appears beyond reach. In 2024, Congress attempted to revive ADPPA with a successor bill titled the American Privacy Rights Act (APRA)—another bipartisan bill with wide support—at least as initially drafted.[143] After significant revisions gutting its protections, however, the bill became unpopular. As one reporter summarized, "[e]veryone hates it."[144]

Because of these revisions, civil liberty groups which initially supported the APRA now advocate killing the bill.[145] Given the lackluster enthusiasm from both parties and the revisions subverting its intended use, the APRA seems unlikely to pass. The APRA represents yet another missed opportunity to enact comprehensive privacy reform at the federal level.

In response to federal inaction, states have increasingly passed their own comprehensive privacy laws, with a total of nineteen states enacting new privacy laws.[146] States have been forced to pick up Congress' slack, leading to patchwork framework of competing privacy laws. Such a patchwork framework will inevitably complicate privacy enforcement and regulations—an already complicated field of law—due to variations in state law. Federal intervention remains necessary.

CONCLUSION

The problems with the SCA have gone unaddressed for decades. As digital technology progressed and became mainstream, the issues with the SCA became even more pronounced. *Carpenter* represents the culmination of the tensions stemming from the SCA's unworkable structure. Post-*Carpenter*, the SCA as it exists can no longer function.

---

[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] The American Privacy Rights Act, H.R. 8188, 118th Cong. (2024); *The American Privacy Rights Act Puts People in Control of Their Data*, Energy & Commerce (Apr. 23, 2024), https://energycommerce.house.gov/posts/the-american-privacy-rights-act-puts-people-in-control-of-their-data.
[144] Dell Cameron, *Surprise! The Latest 'Comprehensive US Privacy Bill Is Doomed*, WIRED (Jun. 27, 2024), https://www.wired.com/story/apra-privacy-bill-doomed/.
[145] *Id.*
[146] *U.S. State Privacy Legislation Tracker,* IAPP (July 22, 2024), https://iapp.org/resources/article/us-state-privacy-legislation-tracker/ [https://perma.cc/A2GM-XDPU].

Congress has two options: let the SCA die the death of a thousand cuts in the courts, or reform the SCA. Adjusting the SCA remains the more logical and cost-effective solution. But considering the congressional inaction for the last decade regarding the SCA and privacy rights generally, a logical and cost-effective solution seems like a pipe dream.