A Poor Craftsman Blames His Tools: Resolving the Potential Post-*Carpenter* Problem in Using the Stored Communications Act to Issue Extraterritorial Warrants

Jordan E. Carlson[*]

ABSTRACT: The privacy pendulum is swinging in favor of greater Fourth Amendment protections after a string of recent Supreme Court cases culminating in the 2018 ruling in Carpenter v. United States. *This precedent-shifting case places the Fourth Amendment in a digital privacy landscape long occupied by one player: the Stored Communications Act. The Carpenter opinion enters the field of digital privacy at a time when certain disputes, particularly those concerning the Fourth Amendment, still engulf the Stored Communications Act. This Note analyzes one of these disputes—the issuance of extraterritorial warrants in accordance with the SCA—in light of the potential for expanded Fourth Amendment protections post-*Carpenter. *After determining whether a risk to current precedent exists, this Note advocates for a revision to the Federal Rules of Criminal Procedure to bring a stop to litigation with potentially disastrous outcomes.*

[*] J.D. Candidate, The University of Iowa College of Law, 2026; B.A., Political Science and International Relations, Truman State University, 2023. I am thankful for the support of my peers on the *Iowa Law Review*, particularly Jack King, Spencer Clark, and Sam Reynoldson for their help in turning this publication into what it is today. A further thank you to Professor Megan Graham for introducing me to this subject and answering my unrelenting questions early in the writing process. Above all else, I am thankful for my parents. A footnote is not nearly long enough to express what your unwavering support means to me.

INTRODUCTION

In 2018, the Supreme Court issued its latest opinion in a string of digital privacy cases, holding for the first time that information provided to a third party can still be constitutionally protected by the Fourth Amendment.[1] *Carpenter v. United States*[2] was heralded as a victory for privacy advocates of all varieties,[3] but it represented something greater for those invested in the rapidly-advancing field of cybersecurity: Uniform national change was coming to the Stored Communications Act ("SCA").[4] The Electronic Communications Privacy

1. Paul Ohm, *The Many Revolutions of* Carpenter, 32 HARV. J.L. & TECH. 357, 358 (2019) ("For the first time, the Court has held that the police must secure a warrant to require a business to divulge information about its customers compiled for the business's purposes, reinventing the reasonable expectation of privacy test and significantly narrowing what is known as the third-party doctrine.").

2. *See generally* Carpenter v. United States, 138 S. Ct. 2206 (2018).

3. *See, e.g.*, Nathan Freed Wessler, *The Supreme Court's Groundbreaking Privacy Victory for the Digital Age*, ACLU (June 22, 2018), https://www.aclu.org/news/privacy-technology/supreme-courts-groundbreaking-privacy-victory-digital-age [https://perma.cc/V34A-BMPA] ("The Supreme Court on Friday handed down what is arguably the most consequential privacy decision of the digital age, ruling that police need a warrant before they can seize people's sensitive location information stored by cellphone companies.").

4. 18 U.S.C. ch. 121 (2018); *see, e.g.*, Richard McCutcheon, *Impractical and Unconstitutional: The Stored Communications Act Post-*Carpenter, HARV. NAT'L SEC. J. ONLINE (Oct. 17, 2024), https://journals.law.harvard.edu/nsj/wp-content/uploads/sites/82/2024/10/McCutcheon-Final-Revisions-Upload.pdf [https://perma.cc/Y4YM-TQPX] (arguing the SCA should be amended in the wake of *Carpenter* to prevent Fourth Amendment violations).

Act of 1986[5]—the omnibus bill that houses the SCA—represented a massive leap forward for cybersecurity at the time it was passed.[6] Unsurprisingly, however, the "outdated communications privacy law . . . fails to address many issues created by technologies that were unimaginable to Congress in the 1980s."[7]

As might be expected from forty-year-old digital privacy legislation, the SCA has repeatedly found itself at the center of litigation.[8] Although some disputes concern relatively narrow issues that squarely fall under the umbrella of the SCA,[9] parties have raised—and courts have found—Fourth Amendment violations housed within the Act.[10] Prior to 2018, however, the lone example of a federal appellate court finding a Fourth Amendment violation in the SCA was *United States v. Warshak*.[11] Under § 2703 of the SCA, law enforcement is allowed multiple avenues to search an individual's electronic communications without a warrant.[12] The Sixth Circuit found that emails, the form of electronic communications at issue in *Warshak*, are protected by a reasonable expectation of privacy and can only be obtained through a validly issued warrant.[13] However, "at present *Warshak* remains closer to a lonely outlier than to a representation of consensus."[14] Prior to *Carpenter*, every constitutional challenge to the SCA—other than *Warshak*—failed at the federal appellate level.[15]

5. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. chs. 65, 109, 119, 121, 205, 206).

6. *Cf.* Emile Ayoub & Elizabeth Goitein, *Closing the Data Broker Loophole*, BRENNAN CTR. FOR JUST. (Feb. 13, 2024), https://www.brennancenter.org/our-work/research-reports/closing-data-broker-loophole [https://perma.cc/M9QM-7U54] ("Much of the ECPA was ahead of its time . . . .").

7. *Id.*

8. *See, e.g.*, Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 874 (9th Cir. 2002) ("[T]he difficulty is compounded by the fact that the ECPA was written prior to the advent of the Internet and the World Wide Web. As a result, the existing statutory framework is ill-suited to address modern forms of communication like Konop's secure website. Courts have struggled to analyze problems involving modern technology within the confines of this statutory framework, often with unsatisfying results.").

9. *See, e.g.*, Sewell v. Bernardin, 795 F.3d 337, 338 (2d Cir. 2015) (unauthorized access to electronic communications); Republic of the Gambia v. Facebook, Inc., 575 F. Supp. 3d 8, 11 (D.D.C. 2021) (disclosures made by service providers); Joseph v. Carnes, 108 F. Supp. 3d 613, 614 (N.D. Ill. 2015) (workplace privacy and email monitoring dispute).

10. *See, e.g.*, United States v. Warshak, 631 F.3d 266, 282, 288 (6th Cir. 2010) ("We find that the government *did* violate Warshak's Fourth Amendment rights by compelling his Internet Service Provider ('ISP') to turn over the contents of his emails."); Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).

11. *Warshak*, 631 F.3d at 282, 288.

12. 18 U.S.C. § 2703.

13. *Warshak*, 631 F.3d at 282–83, 288 ("Accordingly, we hold that a subscriber enjoys a reasonable expectation of privacy in the contents of emails [sent using an Internet Service Provider]. . . . Moreover, to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional.").

14. Walker v. Coffey, 905 F.3d 138, 148 (3d Cir. 2018).

15. *Warshak*, 631 F.3d at 289 ("[T]he Stored Communications Act has been in existence since 1986 and to our knowledge has not been the subject of any successful Fourth Amendment challenges, in any context, whether to § 2703(d) or to any other provision." (quoting Warshak v.

One area of the SCA that has been repeatedly litigated is its grant of power to judges to issue warrants for searches conducted on property outside of their jurisdictions.[16] These extraterritorial warrants directly conflict with Rule 41 of the Federal Rules of Criminal Procedure ("FRCRMP"), a Rule designed to protect the Fourth Amendment.[17] Under Rule 41(b)(1), judges may only issue warrants for "a person or property located within the district."[18] Under the Rules, Rule 41(b)(1) governs unless one of the exceptions—located in Rules 41(b)(2)–(6)—are implicated.[19] Currently, federal circuit courts to rule on the issue have found unanimously that the SCA trumps the FRCRMP.[20]

This Note argues that, in the wake of *Carpenter*'s expansion of the Fourth Amendment into cybersecurity, Rule 41(b) should be amended to conform to the extraterritorial searches permitted by the SCA. Part I of this Note explains how the conflict between the SCA and Rule 41(b) came into existence as well as how the conflict is currently being reconciled. Part II describes the Supreme Court's *Carpenter* decision and how, if at all, it changes the analysis that needs to be performed when issuing an out-of-jurisdiction warrant. Lastly, Part III proposes an amendment to the FRCRMP to ensure that, in the wake of *Carpenter*, no court finds the extraterritorial warrants issued pursuant to the SCA insufficient to protect the Fourth Amendment.

I. THE CREATION OF AN UNDERLYING PROBLEM

This Part will begin by analyzing the creation of the SCA as well as the acceptance of the extraterritorial language contained in 18 U.S.C. 2703(a) and 18 U.S.C. 2703(b)(1)(A). Focus will then shift to Rule 41(b) of the FRCRMP, with an emphasis on resolving unanswered constitutional questions. After exploring the SCA and FRCRMP in Sections I.A and I.B respectively, Section I.C will evaluate the tension between the SCA's grant of extraterritorial warrants and Rule 41(b)'s rejection of the same concept. Section I.C will conclude with how that tension resolved in near unanimous fashion in favor of the SCA.[21]

United States, 532 F.3d 521, 531 (6th Cir. 2008))); *see, e.g.*, United States v. Graham, 824 F.3d 421, 427–28 (4th Cir. 2016) (holding third-party doctrine applied to exclude information covered by the SCA from Fourth Amendment protection).

16. *See* 18 U.S.C. § 2703(a), (b)(1)(A).

17. *See* FED. R. CRIM. P. 41; *infra* notes 74–76 and accompanying text.

18. FED R. CRIM. P. 41(b)(1).

19. *See id.* 41(b)(2)–(6).

20. *See* United States v. Bansal, 663 F.3d 634, 662 (3d Cir. 2011) ("Bansal contends that Rule 41(b), which limits a Magistrate Judge's jurisdiction to the District in which he or she sits, trumps § 2703(a). We, along with other courts to consider the question, reject that contention.").

21. *See infra* Section I.C.

A. *CREATING A "DIGITAL FOURTH AMENDMENT"*

As the United States enters the mid-twenty-first century, it is increasingly difficult to find a facet of life that does not involve the use of technology. Even activities purposefully undertaken for the sake of escaping technology are infiltrated by ease-of-life applications or societal pressure to upload photographs to social media platforms such as Instagram or Facebook.[22] However, some of the most pervasive uses of modern technology have already existed for decades, going so far as to spur legislative innovation to provide regulation in these novel or once-novel areas.[23] Perhaps the best example of this—both in terms of its innovation and pervasiveness[24]—is the ability to communicate with one another entirely through the internet.[25] This ability drastically increased the interconnectedness of the United States, but it also exposed flaws in applying pre-SCA privacy protections to material stored electronically.[26]

Before the enactment of the SCA, digital communications were reliant on protection from the Fourth Amendment; however, whether the Fourth Amendment extended to this new form of communication was uncertain.[27] The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[28] In *Katz v. United States*, the Court determined that an individual has a Fourth Amendment interest when they have a "(subjective) expectation of privacy . . . that society is prepared to recognize as 'reasonable.'"[29] Regardless

22. *See, e.g.*, Linnea Turner, *Does Technology Have a Place in the Outdoors?*, MEDIUM (Jan. 24, 2023), https://medium.com/@turn0436/does-technology-have-a-place-in-the-outdoors-95ad5d493b5c (on file with the *Iowa Law Review*) (addressing the author's feeling that technology has created "a forced change" when participating in outdoor activities).

23. *See, e.g.*, GERALD L. DILLINGHAM, U.S. GOV'T ACCOUNTABILITY OFF., GAO-14-285T, FAA REAUTHORIZATION ACT: PROGRESS AND CHALLENGES IMPLEMENTING VARIOUS PROVISIONS OF THE 2012 ACT 2 (2014), https://www.gao.gov/assets/gao-14-285t.pdf [https://perma.cc/MZB3-KMDF] ("[G]iven the potential and opportunities afforded by new [drone] technologies, the 2012 Act included several provisions with respect to FAA safely integrating [drones] into [national airspace]."); *see also* U.S. GOV'T ACCOUNTABILITY OFF., GAO-24-106122, FEDERAL REGULATION: SELECTED EMERGING TECHNOLOGIES HIGHLIGHT THE NEED FOR LEGISLATIVE ANALYSIS AND ENHANCED COORDINATION (2024), https://www.gao.gov/assets/gao-24-106122.pdf [https://perma.cc/JG8C-A3KR] (providing an overview of the rulemaking process before addressing new technologies that might require the promulgation of regulations).

24. Cal Newport, *E-Mail Is Making Us Miserable*, NEW YORKER (Feb. 26, 2021), https://www.newyorker.com/tech/annals-of-technology/e-mail-is-making-us-miserable (on file with the *Iowa Law Review*).

25. *See* City of Ontario v. Quon, 560 U.S. 746, 760 (2010) ("[Digital] communications are so pervasive that some persons may consider them to be essential means or necessary instruments for self-expression, even self-identification.").

26. 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, 1209–13 (2004).

27. *Id.* at 1210.

28. U.S. CONST. amend. IV.

29. Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy

of whether an individual can meet the burden set out in *Katz*, the protections provided by the Fourth Amendment are void if the individual discloses the protected information to a third party.[30] This waiver of any reasonable expectation of privacy, dubbed the "third-party doctrine," stands true even if the individual discloses the information for a limited purpose or they disclose it to a third party with the expectation that the third party will not further disclose that information.[31] In sum, the Fourth Amendment does not protect information that is disclosed to a third party. An individual seeking protection for information that has been disclosed to a third party will have to find that protection elsewhere.

Under the pre-SCA framework, information communicated electronically would have been, almost by default, exclusively placed under the heading of the third-party doctrine.[32] The Supreme Court's decisions in *United States v. Miller* and *Smith v. Maryland* blended to form a reality in which "business records owned and maintained by a third-party business" required nothing more than a subpoena to access.[33] This holding, as applied to digital information, is still reinforced post-SCA under the theory that internet service providers (ISPs) exist as an intermediary between the sender and receiver of digital information.[34] For example, the telephone records of an individual under investigation can be secured without a warrant because those telephone records have been "voluntarily" turned over to an ISP such as Verizon or T-Mobile.[35] In line with the Court's interpretation of the third-party doctrine, an individual loses their claim to Fourth Amendment protection once their cellphone records are recorded by the ISP.

Foreseeing how the Fourth Amendment was not equipped to provide ample privacy protection in a time where information frequently gets shared to third parties, Congress passed the SCA in 1986.[36] The SCA addressed these privacy concerns by enacting a set of regulatory protections that filled in some of the gaps that needed to be bridged so long as the Fourth Amendment was

and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"); *see* Smith v. Maryland, 442 U.S. 735, 740 (1979) (inquiring whether an individual has a Fourth Amendment interest turns on the test outlined in *Katz*).

30. United States v. Miller, 425 U.S. 435, 443 (1976) ("This Court has held repeatedly that the Fourth Amendment does not prohibit the obtaining of information revealed to a third party and conveyed by him to Government authorities, even if the information is revealed on the assumption that it will be used only for a limited purpose and the confidence placed in the third party will not be betrayed.").

31. *Id.*

32. *See* Kerr, *supra* note 26, at 1209–11.

33. United States v. Davis, 785 F.3d 498, 507–09 (11th Cir. 2015).

34. Kerr, *supra* note 26, at 1210.

35. *See generally* Rehberg v. Paulk, 611 F.3d 828 (11th Cir. 2010) (holding that plaintiff's telephone records were secured through the issuance of subpoenas to plaintiff's cellphone provider).

36. *See* JIMMY BALSER, CONG. RSCH. SERV., LSB10801, OVERVIEW OF GOVERNMENTAL ACTION UNDER THE STORED COMMUNICATIONS ACT (SCA) 2 (2022).

understood not to apply.[37] In doing so, the SCA "create[d] a set of Fourth Amendment-like privacy protections" that outlined limits and procedures to what actions the government had available to them when seeking information from ISPs.[38] In short, the SCA helped ensure privacy protections in two ways: It limited the "government's ability to compel" ISPs to turn over information relating to their customers[39] and it limited the ISP's ability to willingly disclose information pertaining to their clients to the government.[40]

To conclude, the SCA was enacted as a stand-in for the Fourth Amendment at a time in which the Fourth Amendment's application to digital communications was unclear. This lack of clarity stemmed largely from the third-party doctrine which, as applied to digital communications, saw ISPs as third parties rather than mere service providers. Instead of signaling that the third-party doctrine does not apply to ISPs in the digital communication context, the SCA was passed with the opposite understanding. As will be discussed in the next Section, the result was potentially undercutting the protection that the Fourth Amendment may have otherwise provided by drawing attention away from the Constitution and toward the statutory text. As such, the SCA created a set of procedures similar—but not identical—to those emanating from the Fourth Amendment.

1. Implementing the SCA

By providing clear statutory language, the SCA shifted the focus of litigators away from potential constitutional violations and toward the Act itself.[41] Questions that would, at least at face value, invoke the Fourth Amendment were resolved by applying the SCA.[42] One example is the modern analysis performed by courts determining whether individuals have a reasonable expectation of privacy in their "noncontent" information conveyed to ISPs through electronic communications.[43]

While "content" information can be best understood as the actual text of an electronic communication (the body of an email, for example), "noncontent" information encapsulates everything surrounding the email itself. This includes the user's email address, IP address, birthdates, passwords, addresses, and other relevant information the user might have turned over when creating

37. *Id.*

38. Kerr, *supra* note 26, at 1212.

39. *Id.*; 18 U.S.C. § 2703.

40. 18 U.S.C. § 2702; Kerr, *supra* note 26, at 1212–13.

41. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1025 (2010) ("[T]he existence of clear statutory protections has likely drawn attention away from possible constitutional challenges.").

42. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2226 (2018) (Kennedy, J., dissenting) (indicating that each "Court of Appeals to have considered the question" of whether CSLI is protected under the Fourth Amendment has held against applying the constitutional protection and have instead relied on the SCA).

43. *See, e.g.*, United States v. Perrine, 518 F.3d 1196, 1204–05 (10th Cir. 2008).

an account with an ISP.[44] By 2008, "[e]very federal court to address" whether a defendant held a reasonable expectation of privacy in noncontent information "held that subscriber information . . . [was] not protected by the Fourth Amendment's privacy expectation."[45] To see how courts got to such a unanimous position, it is important to see how this precedent evolved.

The courts began by determining that the passage of the SCA was not a legislative indication that Congress desired individuals to possess a reasonable expectation of privacy for stored communications.[46] Rather, the opposite was determined to be true.[47] As cases concerning privacy interests in electronic communications became more common, the determination was made that the SCA "does not create a reasonable expectation of privacy in [noncontent] information."[48] Of course, this did not end the courts' inquiry into whether someone possessed a reasonable expectation of privacy in noncontent information. This determination merely informed courts that the traditional two-pronged *Katz* test was still relevant to determining a privacy interest in noncontent information.[49]

Once courts began applying the *Katz* test to noncontent information, it was quickly apparent that the third-party doctrine would rule the day.[50] During the 1990s and early 2000s, courts had to find a way to apply standards for determining whether a reasonable expectation of privacy existed. To do this, some courts simply applied the third-party doctrine as it had been applied to letters and packages as far back as 1877.[51] In doing so, they held that noncontent information—similar to the information on the outside of a package or on the outside of an envelope—was not protected by a reasonable expectation of privacy.[52] Other courts to take up noncontent information cases established similar precedent by likening noncontent information to the information turned over to a bank when opening a bank account.[53] By comparing noncontent information to the information given to a bank, the court in *Guest* found that "the system operator" was a third party just as a bank teller handling client information was also a third party.[54]

44. Guest v. Leis, 255 F.3d 325, 335 (6th Cir. 2001); *see* Kerr, *supra* note 26, at 1219–20.

45. *Perrine*, 518 F.3d at 1204.

46. United States v. Hambrick, 55 F. Supp. 2d 504, 507 (W.D. Va. 1999) ("[T]he ECPA is hardly a legislative determination that this expectation of privacy is one that rises to the level of 'reasonably objective' for Fourth Amendment purposes.").

47. *Id.*

48. *Id.*

49. *See id.* at 508; *Guest*, 255 F.3d at 335; United States v. D'Andrea, 497 F. Supp. 2d 117, 120–21 (D. Mass. 2007); Freedman v. Am. Online, Inc., 412 F. Supp. 2d 174, 181 (D. Conn. 2005).

50. *See* United States v. Perrine, 518 F.3d 1196, 1204 (10th Cir. 2008).

51. United States v. Forrester, 512 F.3d 500, 511 (9th Cir. 2008) (referring to *Ex parte* Jackson, 96 U.S. 727, 733 (1877)).

52. *Id.*

53. *Guest*, 255 F.3d at 336.

54. *Id.*

These early cases had a profound impact on creating the precedent that is now applied to modern SCA cases, regardless of how antiquated that standard might seem. Instead of engaging in a good-faith Fourth Amendment analysis, modern courts have been willing to accept the simple-to-grasp conclusions that stem from *Ex parte Jackson* and *Guest*. In 2018, for example, an individual's noncontent information relating to his Facebook account was gathered through an SCA-compliant subpoena.[55] When the individual challenged the constitutionality of such a search, the court found that it was a matter of "routine[]" to reject such an argument because of the lack of privacy expectation.[56] As recently as 2023, courts have held that they "need not reach the question of whether [defendant] has a reasonable expectation of privacy in [noncontent information]" given that it was gathered in compliance with an SCA subpoena.[57]

These modern cases demonstrate that SCA precedent regarding noncontent information has become powerful enough for courts to conclude that meaningful Fourth Amendment analysis on the issue is no longer warranted. Although courts initially felt the need to perform rather lengthy analyses during the infancy of the SCA and noncontent information, their decisions were informed almost exclusively by cases that dealt with other areas of the law. Those early decisions resulted in precedent that courts now take for granted, regardless of whether the initial reasoning was sound or logically complied with the evolution of technology. As will be looked at extensively with the discussion of *Carpenter* in Part II, there is little reason to expect this trend to change course without Supreme Court intervention.

2. Narrowing Focus: The SCA and Extraterritoriality

The SCA's tolerance for extraterritorial warrants demands attention. The grants of extraterritoriality this Note focuses on appear in § 2703(a) and § 2703(b)(1)(A). The relevant language establishes that law enforcement may require certain ISPs to disclose information compelled by "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a *court of competent jurisdiction*."[58] A "court of competent jurisdiction" is defined in 18 U.S.C. § 2711(3) as:

> (A) any district court of the United States (including a magistrate judge of such a court) or any United States court of appeals that—
>
> (i) has jurisdiction over the offense being investigated;

55. Humphrey v. Dep't of Def., Misc. No. 18-00369, 2018 WL 5020209, at *1 (D. Haw. Oct. 16, 2018).

56. *Id.* at *2.

57. United States v. Peterson, No. 22-00196-01-CR-W-DGK, 2023 WL 5920869, at *5 (W.D. Mo. July 18, 2023).

58. 18 U.S.C. § 2703(a), (b)(1)(A) (emphasis added).

> (ii) is in or for a district in which the provider of a wire or electronic communication service is located or in which the wire or electronic communications, records, or other information are stored; or
>
> (iii) is acting on a request for foreign assistance pursuant to section 3512 of this title;
>
> (B) a court of general criminal jurisdiction of a State authorized by the law of that State to issue search warrants; or
>
> (C) a court-martial or other proceeding under chapter 47 of title 10 (the Uniform Code of Military Justice) to which a military judge has been detailed;[59]

The language relevant for this discussion is included in § 2711(3)(A)(i), which allows magistrate judges to issue search warrants for information stored anywhere in the United States so long as it is relevant to the crime being investigated in the magistrate judge's jurisdiction.[60] Under the status quo, this language has been interpreted as deeming extraterritorial warrants valid.[61] For the reasons set out in Section I.B, allowing extraterritorial warrants might require more considerations than the SCA lets on.

B. APPLYING THE FEDERAL RULES OF CRIMINAL PROCEDURE

The FRCRMP took effect in 1946, a time in which "[t]he need for standardized procedures in a uniform system was obvious."[62] To provide such uniformity, the Rules "govern all criminal proceedings in the federal courts,"[63] with the intention of "provid[ing] . . . the just determination of every criminal proceeding, to secure simplicity in procedure and fairness in administration, and to eliminate unjustifiable expense and delay."[64] An essential aspect of ensuring these goals are met, particularly the fairness in administration, is to make certain the proceedings, as governed by the Rules, will comply with the Constitution.[65] While not every rule is promulgated with the Constitution in mind, certain rules exist at least in part to ensure that criminal proceedings unfold in a manner that poses the least risk of violating the Constitution.[66]

---

59. *Id.* § 2711(3).

60. *Id.*

61. *See, e.g.*, United States v. Berkos, 543 F.3d 392, 397 (7th Cir. 2008).

62. 1 CHARLES ALAN WRIGHT & ANDREW D. LEIPOLD, FEDERAL PRACTICE AND PROCEDURE: FEDERAL RULES OF CRIMINAL PROCEDURE § 1 (5th ed. 2022).

63. *Id.*

64. FED. R. CRIM. P. 2.

65. *See* Giordenello v. United States, 357 U.S. 480, 485 (1958) ("The provisions of [the Federal Rules of Criminal Procedure] must be read in light of the constitutional requirements they implement.").

66. *See* McCarthy v. United States, 394 U.S. 459, 465 (1969) ("[Rule 11] is designed to assist the district judge in making the constitutionally required determination that a defendant's guilty

One of the relevant provisions for implementing the Fourth Amendment is Rule 41.[67] Rule 41(b)(1) requires a magistrate judge issuing a warrant preside over the location of the person or property being targeted in the warrant.[68] After laying out this general rule, Rule 41(b)(1) is followed by Rules 41(b)(2), (3), (4), (5), and (6), with each rule listing an exception to the territoriality requirement.[69] For example, these exceptions include cases involving terrorism or the installation of a tracking device.[70] This Note is primarily concerned with just the text of Rule 41(b)(1), which gives magistrate judges the "authority to issue a warrant to search for and seize a person or property located within the district" they occupy.[71] It is important to recognize that there are other provisions of Rule 41 that mention accessing data that is being kept in electronic storage; however, these sections are not traditionally implicated in cases involving § 2703(a) or § 2703(b)(1)(A).[72] This point is raised primarily in reference to Rule 41(b)(6)—authorizing a magistrate judge to issue an extraterritorial warrant relating to electronically stored media *only if one of two specific scenarios are met*[73]—and Rule 41(e)(2)(B), which addresses electronically stored information but fails to grant extraterritoriality to the warrant being issued.[74]

A violation of Rule 41 "is not per se an unreasonable search and seizure in violation of the Fourth Amendment."[75] However, to best ensure that a procedural violation does not rise to the level of infringing the defendant's constitutional rights, compliance with Rule 41 is the government's most prudent

plea is truly voluntary. . . . [T]he more meticulously the Rule is adhered to, the more it tends to discourage . . . attacks on the constitutional validity of guilty pleas.").

67. Jones v. United States, 357 U.S. 493, 498 (1958) ("The decisions of this Court have time and again underscored the essential purpose of the Fourth Amendment to shield the citizen from unwarranted intrusions into his privacy. This purpose is realized by Rule 41 . . . which implements the Fourth Amendment . . . ." (citations omitted)); *see also* Matter of Search of Info. Associated with [Redacted]@Mac.com, 13 F. Supp. 3d 157, 164–65 (D.D.C. 2014) ("Rule 41 embodies standards which conform with the requirements of the Fourth Amendment." (quoting United States v. Haywood, 464 F.2d 756, 760 (D.C. Cir. 1972))).

68. FED. R. CRIM. P. 41(b).

69. *See id.* 41(b)(2)–(6).

70. United States v. Horton, 863 F.3d 1041, 1047 (8th Cir. 2017) (explaining the general territoriality requirement of Rule 41(b)(1) and the exceptions "for domestic and international terrorism, for the installation of a tracking device, and for property located outside of a federal district").

71. FED. R. CRIM. P. 41(b)(1).

72. *See, e.g.*, United States v. Bansal, 663 F.3d 634, 662 (3d Cir. 2011) (illustrating that claims arising out of the SCA's extraterritorial language conflict with Rule 41(b)(1)).

73. Under Rule 41(b)(6), an extraterritorial warrant for electronically stored information can be accessed if: (1) "the district where the media or information is located has been concealed through technological means"; or (2) "in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts."

74. FED. R. CRIM. P. 41(e)(2)(B).

75. United States v. Welch, 811 F.3d 275, 280 (8th Cir. 2016).

course of action.[76] In complying with the text of Rule 41, this means having warrants signed by judges presiding over the property in question.

C. *RESOLVING THE CONFLICT: § 2703 TRUMPS RULE 41*

Taking Rule 41(b) and the extraterritorial language of § 2703 together, it is apparent that a conflict exists. Barring exceptions, Rule 41(b) requires that a magistrate judge preside over the area that encapsulates the property being sought by the government.[77] On the other hand, § 2703 grants any court of competent jurisdiction the ability to issue a warrant; this includes magistrate judges that are merely presiding over an offense being investigated.[78] Although such a conflict might be expected to generate disagreement between circuits, courts are unanimous in concluding that § 2703 prevails over Rule 41.[79] Courts resolving the issue have rested their opinions on two grounds: The plain text of § 2703 unambiguously grants courts the authority to issue extraterritorial warrants, and legislative history indicates that extraterritorial warrants were desired by Congress.[80]

Regardless of the subsequent steps courts choose to take when resolving a statutory interpretation question, the first step is to examine whether there is ambiguity in the plain text of the statute.[81] As the relevant statutes in the SCA currently read, warrants must be "issued using the *procedures* described in the Federal Rules of Criminal Procedure."[82]

After performing this initial step, some courts have concluded that the plain text is sufficient to hold § 2703 above Rule 41. Courts that subscribe to this argument agree that Rule 41(b), despite being listed in the Federal Rules of Criminal *Procedure*, is not a procedural rule at all.[83] Rather, courts subscribing to this theory conclude that Rule 41(b) is a substantive provision.[84] In *United States v. Berkos*, the Seventh Circuit—the first of the circuit courts to weigh in on the issue—found that for a rule to be procedural, it must address "procedures to be used for issuing the warrant" not just "the circumstances as

76. *See, e.g.*, United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017) (demonstrating that, but for the Rule 41 violation, the analysis as to whether a Fourth Amendment violation occurred would not have proceeded).

77. FED. R. CRIM. P. 41(b)(1).

78. 18 U.S.C. § 2703(a), (b)(1)(A); *id.* § 2711(3).

79. *See* United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022) ("[T]hree circuits have ruled that warrants issued pursuant to the SCA are exempted from the venue limitation of Rule 41(b), and no circuit has ruled to the contrary.").

80. *See* United States v. Scully, 108 F. Supp. 3d 59, 75–84 (E.D.N.Y. 2015) (summarizing the two primary methods courts have used to resolve the conflict between the SCA's extraterritorial warrants and Rule 41(b)'s territoriality requirement).

81. *See, e.g.*, United States v. Berkos, 543 F.3d 392, 396–97 (7th Cir. 2008).

82. 18 U.S.C. § 2703(a), (b)(1)(A) (emphasis added).

83. *Berkos*, 543 F.3d at 398 ("Rule 41(b) deals with substantive judicial authority—not procedure—and thus does not apply to § 2703(a).").

84. *Id.*

to when a court may issue a warrant."[85] Without providing more analysis on the subject, the Third Circuit in *United States v. Bansal* agreed with the Seventh Circuit and upheld an identical holding regarding extraterritoriality.[86]

In *United States v. Ackies*, the First Circuit agreed with the reasoning supplied by its sister circuits, but went a step further to address the legislative history and intent employed by some federal district courts to arrive at the same conclusion.[87] After all, at least one federal district court found the phrase "using the procedures described in [Rule 41]" unclear, suggesting that perhaps the language was not as unambiguous as other courts perceived it to be.[88] Under the opinion of the courts that analyzed legislative intent, the development of § 2703(a) from its pre-Patriot Act language to its present language was dispositive of the ambiguity issue.[89]

Following the passage of the Patriot Act in 2001, the language of § 2703(a) was amended in two ways. First, prior to the Patriot Act, § 2703(a) required the government to acquire a "warrant issued *under* the Federal Rules of Criminal Procedure or equivalent state warrant,"[90] suggesting that the issuing court had to comply with all of the FRCRMP, including Rule 41's territoriality requirement. Once the Patriot Act amendments were enacted, § 2703 only required search warrants to be issued "*using the procedures* described in the Federal Rules of Criminal Procedure,"[91] suggesting that at least some rules in the FRCRMP were not procedural. The new "using the procedures" language was further bolstered by the second change brought about by the Patriot Act: adding that "court[s] with jurisdiction over the offense under investigation" were permitted to issue warrants.[92] Taken in conjunction, the Patriot Act amendments made clear to skeptical courts that § 2703 is a grant to issue extraterritorial warrants.[93]

The First Circuit's summary of the conflict between § 2703 and Rule 41(b) in *Ackies* was the first true survey of the legal landscape performed by a federal appellate court since the Seventh Circuit's decision in *Berkos* eleven years earlier. Accordingly, the Second Circuit's decision in *United States v.*

85. *Id.*

86. United States v. Bansal, 663 F.3d 634, 662 (3d Cir. 2011) ("Bansal contends that Rule 41(b), which limits a Magistrate Judge's jurisdiction to the District in which he or she sits, trumps § 2703(a). We, along with other courts to consider the question, reject that contention.").

87. United States v. Ackies, 918 F.3d 190, 201–03 (1st Cir. 2019).

88. *In re* Search Warrant, 362 F. Supp. 2d 1298, 1302 (M.D. Fla. 2003) ("The words 'by a court with jurisdiction over the offense under investigation' do not authorize out-of-district warrants in non-terrorism cases. Courts without jurisdiction over the offense under investigation have never been authorized to issue warrants.") (citation omitted), *rev'd*, No. 6:05-MC-168-Orl-31JGG, 2005 WL 3844032 (M.D. Fla. Feb. 13, 2006).

89. *Ackies*, 918 F.3d at 201–02 (rejecting the argument that Rule 41 applies in its entirety).

90. 18 U.S.C. § 2703(a) (2000) (emphasis added).

91. Patriot Act, Pub. L. No. 107-56, § 220(a)(1), 115 Stat. 272, 291–92 (2001).

92. *Id.* § 220, 115 Stat. at 291–92.

93. *See, e.g.*, *In re* Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971, at *2–7 (D. Ariz. May 21, 2007).

Guzman Loera came just three years after *Ackies* and found "that geographical limitations of Rule 41(b) do not apply to warrants issued under SCA § 2703 for essentially the same reasons set forth in [*Ackies*, *Bansal*, and *Berkos*]."[94]

In sum, the federal appellate courts to address the question have held unanimously that the grant of extraterritoriality found in § 2703 supersedes the territoriality requirement of Rule 41(b) of the FRCRMP. These holdings come primarily on the shoulders of a plain text analysis of § 2703(a) or by examining the development of the SCA after the passage of the Patriot Act. This Note will now turn to its central focus: How, if at all, might the Supreme Court's decision in *Carpenter* alter the relationship between § 2703 and Rule 41(b)?

II. *CARPENTER* AND EXPANDING THE REASONABLE EXPECTATION OF PRIVACY

This Part will begin by summarizing the circuit court decisions that analyzed the acquisition of cell-site location information under the SCA before 2018. After analyzing those opinions, attention will shift to the Supreme Court's interpretation of the issue in *Carpenter*. Analysis of *Carpenter* will focus primarily on the shift in precedent regarding the reasonable expectation of privacy as it applies to the third-party doctrine. From there, this Note will question whether courts should still be allowing extraterritorial warrants in the event the Fourth Amendment applies to the SCA, and what the impact of leaving this problem unaddressed might be. Finally, this Part will propose an amendment to Rule 41 to avoid any unanticipated adverse effects of the *Carpenter* opinion.

A. *BUILDING UP TO* CARPENTER

Under § 2703(d) of the SCA, law enforcement may be granted a court order compelling disclosure of the "contents of a wire or electronic communication" if law enforcement offers "specific and articulable facts showing that there are reasonable grounds to believe that [such information] . . . [is] relevant and material to an ongoing criminal investigation."[95] Orders issued under § 2703(d) ("D orders") have been used to gather, among many other things, messages sent from Twitter accounts,[96] the content of emails,[97]

94. United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022).

95. 18 U.S.C. § 2703(d).

96. *In re* U.S. for an Order Pursuant to 18 U.S.C. Section 2703(d), 707 F.3d 283, 287 (4th Cir. 2013) ("Specifically, the order directed Twitter to provide [Appellants'] names, usernames, personal contact information, account information, connection records, financial data, length of service, direct messages to and from email addresses and Internet Protocol addresses for all communications between November 1, 2009, and December 14, 2010.").

97. United States v. Hanna, 661 F.3d 271, 287 n.4 (6th Cir. 2011) ("The law in effect at that time provided that a governmental entity need not obtain a warrant for such emails, but instead could compel an internet service provider to disclose the contents of email communications at least 180 days old through a simple subpoena.").

and past phone records[98] all without a warrant.[99] However, if for no other reason than the *Carpenter* decision itself, D orders are most infamous for their ability to grant law enforcement the ability to gather cell site location information ("CSLI") with a court order.[100]

CSLI is "a time-stamped record" of a user's location, a "record" that is generated each time a cellphone scans for a signal.[101] This scan typically occurs multiple times per minute, with some scans being as frequent as every seven seconds.[102] The precision of the scan can vary greatly and is dependent on the density of cellphone towers in a cellphone's vicinity.[103] In areas containing more cellphone towers—typically those that are urban and more densely populated—the accuracy of CSLI can place a cellphone within a two hundred foot area.[104] That area can be reduced down to fifty feet if the cell phone has GPS capabilities and reduced down to less than six feet if "the cell phone carrier is asked by a law enforcement agency to track, prospectively, the location of a cell phone."[105]

CSLI is generally stored by a cell service provider, allowing law enforcement to seek information for a cellphone's whereabouts after the fact.[106] Although the storage period was initially for a period of weeks, cell service companies "saw the potential for huge profits by monetizing such location data" and "mov[ed] toward longer retention periods" as "the costs of data storage . . . plummet[ted]."[107] By the time of the *Carpenter* decision, cell service providers were holding on to CSLI for periods of greater than a year.[108] However, if more than a year's worth of location data was insufficient, some D orders were forward-looking.[109] D orders can go so far as to give law enforcement real-time updates on a cellphone's location by having the cell service provider "ping" the phone's location and immediately relay that data to law enforcement.[110]

98. United States v. Terry, 572 F.3d 430, 432 (7th Cir. 2009) ("On the same day, acting pursuant to 18 U.S.C. § 2703(d), they also obtained 5638's past phone records.").

99. *See supra* notes 77–80.

100. *See, e.g.*, Susan Freiwald & Stephen Wm. Smith, *The* Carpenter *Chronicle: A Near-Perfect Surveillance*, 132 HARV. L. REV. 205, 211–16 (2018).

101. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

102. *Id.*; State v. Earls, 70 A.3d 630, 632 (N.J. 2013).

103. *See Carpenter*, 138 S. Ct. at 2211–12; *In re* U.S. for an Ord. Directing a Provider of Elec. Commc'n Serv. to Disclose Recs. to the Gov't, 534 F. Supp. 2d 585, 590 (W.D. Pa. 2008) [hereinafter *In re U.S. for an Order*].

104. *In re U.S. for an Order*, 534 F. Supp. 2d at 590.

105. *Id.*; Commonwealth v. Princiotta, No. 2009-00965, 2013 WL 1363901, at *3 (Mass. Super. Ct. Apr. 1, 2013).

106. *See Princiotta*, 2013 WL 1363901, at *3.

107. Freiwald & Smith, *supra* note 100, at 213–14.

108. *Id.* at 213.

109. *See In re* Application of U.S. for an Ord. Authorizing Disclosure of Location Info. of a Specified Wireless Tel., 849 F. Supp. 2d 526, 531 (D. Md. 2011).

110. *See id.*

Before the Supreme Court's decision in *Carpenter*, law enforcement could secure a defendant's CSLI from a service provider without a warrant because, under the third-party doctrine, the defendant had voluntarily turned that information over to the provider when they made or received phone calls.[111] Though at least one district court was hesitant in applying the third-party doctrine to the use of CSLI,[112] it was not long before the Fifth Circuit held D orders to be a valid means for acquiring historical CSLI.[113] Within four years of the Fifth Circuit's decision, four other circuit courts arrived at the same conclusion: Historical CSLI was available to law enforcement by means of a D order.[114] Despite unanimity from the appellate courts that had taken up the CSLI issue, the Supreme Court agreed to review *Carpenter*, the Sixth Circuit's ruling from 2016.

Although the facts of each D order case are unique in regard to which parties are involved, the facts of *Carpenter* help illustrate how influential material gathered under the SCA can be. In this case, historical CSLI was acquired pursuant to a D order after a string of Radio Shack and T-Mobile stores were robbed in Detroit, Michigan.[115] One suspect admitted to the FBI that there had been fifteen accomplices who assisted in a series of robberies that spanned Michigan and Ohio over the previous four months.[116] During his conversation with the FBI, the suspect turned over the phone numbers of some of the men involved.[117] Based on the information supplied by the apprehended suspect, the FBI applied for and received D orders for some of the suspects' historical CSLI in an attempt to place them at the locations in which the robberies had occurred.[118] Among the suspects was Timothy Carpenter.[119]

111. United States v. Thompson, 866 F.3d 1149, 1154–55 (10th Cir. 2017).

112. *See In re* Application of U.S. for an Ord. Authorizing Release of Hist. Cell-Site Info., 736 F. Supp. 2d 578, 596 (E.D.N.Y. 2010).

113. *In re* Application of the U.S. for Hist. Cell Site Data, 724 F.3d 600, 615 (5th Cir. 2013) ("Using the proper framework, the SCA's authorization of § 2703(d) orders for historical cell site information if an application meets the lesser 'specific and articulable facts' standard, rather than the Fourth Amendment probable cause standard, is not per se unconstitutional.").

114. *See Thompson*, 866 F.3d at 1160 ("[W]e hold that cell-phone users lack a reasonable expectation of privacy in their historical CSLI, which users voluntarily convey to third-party cell-service providers. Therefore, the district court did not err in granting the government's application for orders requesting historical CSLI under § 2703(d) . . . ."); United States v. Graham, 824 F.3d 421, 426 (4th Cir. 2016) ("The Government followed [§ 2703(d)] and Defendants do not contend that in doing so it failed to meet the requirements of the Act."); United States v. Carpenter, 819 F.3d 880, 890 (6th Cir. 2016) ("In sum, we hold that the government's collection of business records containing cell-site data was not a search under the Fourth Amendment."); United States v. Davis, 785 F.3d 498, 511 (11th Cir. 2015) ("Based on the SCA and governing Supreme Court precedent, we too conclude the government's obtaining a § 2703(d) court order for the production of MetroPCS's business records did not violate the Fourth Amendment.").

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

116. *Id.*

117. *Id.*

118. *Id.*

119. *Id.*

The D orders for Carpenter compelled his wireless service providers to disclose historical CSLI for the four-month period during which the robberies occurred.[120] These orders included the disclosure of the start and end location of all of Carpenter's phone calls during the four-month period as well as a period of two days "when Carpenter's phone was 'roaming' in northeastern Ohio."[121] In total, the FBI was able to acquire almost 13,000 data points over the four-month period, creating a detailed log of "101 data points per day" that mapped where Carpenter had traveled.[122]

After the collection of data, Carpenter was charged with multiple counts of robbery and carrying a firearm during the commission of a federal crime of violence. [123] Carpenter attempted to suppress the CSLI that had been turned over by his wireless providers but these motions were denied by the district court.[124] At trial, the Government argued that the CSLI, which placed Carpenter at the location of four robberies, "clinched the case."[125] The district court evidently agreed with the Government's position, sentencing Carpenter to over one hundred years in prison.[126] As alluded to previously, the Sixth Circuit affirmed the decision of the lower court, finding that Carpenter "lacked a reasonable expectation of privacy in the location information collected by the FBI because he had shared that information with his wireless carriers."[127]

The Supreme Court's decision to grant certiorari garnered significant attention, with some commentators citing its potential to "become the most important electronic-privacy case of the 21st century"[128] because there were indications that the Court was willing to revise the third-party doctrine that the courts of appeals felt bound to apply due to existing SCA precedent.[129] The first of these indications stemmed from the 2012 case *United States v. Jones*. In *Jones*, the Court found unanimously that a Fourth Amendment search had been performed when law enforcement attached a GPS tracking device to an individual's car.[130] This holding disagreed with the findings of the district court, which found that no reasonable expectation of privacy existed when

120. *Id.*

121. *Id.*

122. *Id.*

123. *Id.*

124. *Id.*

125. *Id.* at 2213.

126. *Id.*

127. *Id.*

128. Jeffrey Rosen, *A Liberal-Conservative Alliance on the Supreme Court Against Digital Surveillance*, ATLANTIC (Nov. 30, 2017), https://www.theatlantic.com/politics/archive/2017/11/bipartisanship-supreme-court/547124 (on file with the *Iowa Law Review*).

129. Adam Liptak, *Back at Full Strength, Supreme Court Faces a Momentous Term*, N.Y. TIMES (Oct. 1, 2017), https://www.nytimes.com/2017/10/01/us/politics/supreme-court-term-2017.html (on file with the *Iowa Law Review*).

130. United States v. Jones, 565 U.S. 400, 404 (2012).

the individual was driving on a public street.[131] The second indication that the Court was willing to revise longstanding privacy precedent came in the 2014 decision of *Riley v. California*, a case addressing the warrantless search of data stored on cellphones seized during an arrest.[132] Before the Court's decision, a circuit split existed regarding whether police officers could search cellphones that were incidental to an arrest being made.[133] However, in another unanimous decision, the Court held that police officers are required to receive a warrant before they can search cellphones, regardless of whether the phone was recovered during an otherwise lawful arrest.[134]

The potential for a shift in precedent spurred excitement from organizations such as the American Civil Liberties Union ("ACLU"), the organization that represented Carpenter before the Supreme Court. Nathan Freed Wessler, an ACLU attorney arguing before the Court, commented on the outdated standards being used in modern privacy cases, remarking that "[i]t's 2017, not 1977, . . . people have the right to expect that their everyday movements and thoughts will not be freely available to the government without a warrant."[135] This sentiment was echoed by tech giants often on the receiving end of court orders requiring disclosure of user information[136] as well as twenty media organizations concerned about the ease with which the Government could acquire the location of reporters and their informants.[137]

Given the outcome of privacy cases leading up to the Supreme Court's decision in *Carpenter* and the widespread support for revising the existing third-party precedent, privacy advocates had "reasons for optimism."[138] However, even assuming that the Fourth Amendment did apply to historical CSLI, it remained

131. *Id.* at 402–03.

132. *See generally* Riley v. California, 573 U.S. 373 (2014).

133. *See Riley v. California*, ELEC. PRIV. INFO. CTR., https://epic.org/documents/riley-v-california-2 [https://perma.cc/KK55-5QLH].

134. *Id.*

135. Press Release, Am. C.L. Union, ACLU at Supreme Court Wednesday to Argue in Cellphone Tracking Case (Nov. 27, 2017), https://www.aclu.org/press-releases/aclu-supreme-courtwednesday-argue-cellphone-tracking-case [https://perma.cc/6ZF6-8HJV].

136. Brief for Technology Companies as Amici Curiae in Support of Neither Party at 2–9, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (showing the support of Airbnb, Apple, Box, Cisco Systems, Dropbox, Evernote, Facebook, Google, Microsoft, Mozilla, Nest Labs, Oath, Snap, Twitter, and Verizon).

137. Brief Amici Curiae of the Reporters Committee for Freedom of the Press and 19 Media Organizations in Support of Petitioner at 1–8, Carpenter v. United States, 138 S. Ct. 2206 (2018) (No. 16-402) (showing the support of the Reporters Committee for Freedom of the Press, American Society of News Editors, Associated Press Media Editors, Association of Alternative Newsmedia, First Amendment Coalition, First Look Media Works, Freedom of the Press Foundation, International Documentary Association, Investigative Reporting Workshop, The Media Consortium, Association of Magazine Media, National Press Photographers Association, New England First Amendment Coalition, News Media Alliance, The News Guild, Online News Association, Radio Television Digital News Association, Reporters Without Borders, Society of Professional Journalists, and The Tully Center for Free Speech).

138. Liptak, *supra* note 129.

to be seen how the Court would go about applying it, and on what grounds.[139] This question was answered to questionable satisfaction in the Supreme Court's decision on June 22, 2018.

B. UNITED STATES V. CARPENTER

The Supreme Court granted certiorari to answer the question of whether "the Government conducts a search under the Fourth Amendment when it accesses historical cell phone records that provide a comprehensive chronicle of the user's past movements."[140] By a margin of 5–4, the Court answered that question in the affirmative; holding that "an individual maintains a legitimate expectation of privacy in the record of his physical movements as captured through CSLI."[141] Despite acknowledging that the third-party doctrine of *Smith* and *Miller* would traditionally apply to CSLI just as the circuit courts had held, the Court "decline[d] to extend [the third-party doctrine] to cover these novel circumstances."[142] However, the Court was careful to make clear that this movement away from the third-party doctrine was not abandoning the principle altogether.[143] Instead, the ruling stood more as a retooling of the popular doctrine.

Rather than apply the literal language of *Smith*[144] like courts before it, the Supreme Court relied on the principles underlying *Smith* and *Miller* just as it did when it decided *Riley* four years prior.[145] Unfortunately, the Court failed to sufficiently elaborate on what those principles are, leaving some to observe the majority's "failure to cite any legal scholarship" when ruling on *Carpenter*.[146] Instead, those reading the opinion are supplied with a more generalized description of CSLI and its potential for privacy intrusions, but why those intrusions cross the line of constitutionality is left a mystery.

Not elaborating on what factors are essential to a privacy analysis has left scholars to fill in the gaps from a few informative lines of text scattered throughout the majority's opinion.[147] For example, the Court acknowledges

139. Rosen, *supra* note 128.

140. Carpenter v. United States, 138 S. Ct. 2206, 2211 (2018).

141. *Id.* at 2217.

142. *Id.*

143. *Id.* at 2220.

144. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

145. Freiwald & Smith, *supra* note 100, at 224 ("The Court went back to the principles underlying the third party cases, as it had done in *Riley v. California* with the search-incident-to-arrest exception to the warrant requirement.").

146. Ohm, *supra* note 1, at 370 ("This is meant to address a criticism that has been directed at the majority's opinion: its failure to cite any legal scholarship.").

147. *See, e.g.*, Charlie Brownstein, *Confronting* Carpenter*: Rethinking the Third-Party Doctrine and Location Information*, 92 FORDHAM L. REV. 183, 202–03 (2023) (explaining that the Supreme Court's decision lacked clear guidelines for lower courts); Freiwald & Smith, *supra* note 100, at

that "cell phone tracking is remarkably easy, cheap, and efficient compared to traditional investigative tools."[148] Additionally, "[a] cell phone faithfully follows its owner beyond public thoroughfares and into private residences, doctor's offices, political headquarters, and other potentially revealing locales."[149] Data is also "logged for all of the 400 million devices in the United States," not just those cell phones belonging to individuals under investigation.[150] In fact, the only way to "escape this tireless and absolute surveillance" is to be in the exceptionally small minority of Americans that do not own a cellphone.[151] It is from this variety of descriptions that authors have been left to assemble a workable test and, while there is no way to be certain, some are confident they have deciphered the Court's code.

Professor Susan Freiwald has advocated for a four-factor test to determine whether one's reasonable expectation of privacy has been breached by electronic surveillance since well before CSLI cases began emerging in appellate courts in the 2010s.[152] This four-factor test "evaluat[es] whether [the method of surveillance] is a hidden, intrusive, indiscriminate, and continuous method," a test already applied by federal appellate courts when scrutinizing video surveillance.[153] While analyzing the *Carpenter* decision, Professor Paul Ohm observed that Professor Freiwald's advocacy for the four-factor test "bested the Supreme Court by seven years" given the similarities between the Court's analysis and her own.[154] In her own response to the case, Freiwald was not ignorant to the Court's vague application of the four-factor test.[155] She and Professor Stephen Smith concluded that the Court's decision was driven by whether the acquisition of CSLI was hidden, continuous, indiscriminate, and intrusive, but also how cheap and efficient the acquisition is as well.[156] Smith concluded that, by including the cost and efficiency of the surveillance technique, the Court effectively added a fifth factor to Freiwald's four-factor

219 (explaining that the Court "did not list" the factors they extrapolate as being "central to its holding"); Ohm, *supra* note 1, at 361 (explaining that "[t]he Court did not exhaustively specify or defend the new test" and that to find a new test requires "a close reading of the opinion").

148. Carpenter v. United States, 138 S. Ct. 2206, 2217–18 (2018).

149. *Id.* at 2218.

150. *Id.*

151. *Id.*

152. *See* Susan Freiwald, *First Principles of Communications Privacy*, 2007 STAN. TECH. L. REV. 3, 15–18; *see also* Ohm, *supra* note 1, at 370 ("Freiwald has long advocated that the Court embrace her own four-factor test for deciding whether there is an invasion of [a reasonable expectation of privacy] in electronic surveillance . . . . Using this test, she bested the Supreme Court by seven years, arguing in 2011 that the police should be required to obtain a warrant to access CSLI.").

153. Freiwald, *supra* note 152, at 13.

154. Ohm, *supra* note 1, at 370.

155. Freiwald & Smith, *supra* note 100, at 219–21.

156. *Id.*

test.[157] However, as has been emphasized at length, Freiwald and Smith acknowledge that "the Court did not list these . . . factors explicitly."[158]

Without direct acknowledgement of whether a test exists, it is unclear whether the five factors identified by Professors Freiwald and Smith are truly the test to be taken away from *Carpenter*.[159] One of the few things that was concretely derived from the Court's opinion is that the acquisition of CSLI, which was previously thought to be under the exclusive scope of the SCA, is now entitled to Fourth Amendment protection.[160] For the time being, that leaves the legal world to wonder how broad the reach of *Carpenter* really is and, at least for the sake of this Note, whether it is possible for *Carpenter* to influence the issuance of extraterritorial warrants.[161]

C. *ARE NARROW OPINIONS REALLY NARROW?*

The first hurdle to analyzing whether *Carpenter* has an effect on broader SCA issues outside of CSLI comes from the text of the *Carpenter* opinion itself: "Our decision today is a narrow one."[162] Should the Chief Justice be taken at his word, the clear implication is that *Carpenter*'s expansion of the Fourth Amendment only pertains to historic CSLI data and should not be construed as speaking on any other issues of the SCA or surveillance techniques. To sell the narrowness of the Court's holding, the opinion draws on language from Justice Frankfurter when the Court confronted a question pertaining to technological advancements in the 1940s.[163] In doing so, Chief Justice Roberts writes, "the Court must tread carefully in [cases considering new innovations], to ensure that we do not 'embarrass the future.'"[164] But is the Roberts Court to be trusted when making such a proclamation? History suggests that the answer is no.[165]

157. *Id.* at 219–20 (including "expense and efficiency" as a fifth factor in addition to Professor Freiwald's four that had been established pre-*Carpenter*).

158. *Id.* at 219.

159. Marc Rotenberg, Carpenter *Fails to Cabin* Katz *as* Miller *Grinds to a Halt: Digital Privacy and the Roberts Court*, AM. CONST. SOC'Y (Nov. 28, 2018), https://www.acslaw.org/wp-content/uploads/2019/01/ACS-Supreme-Court-Review-2018-Revised.pdf [https://perma.cc/Q5EX-WWQM] ("The Court has moved the line with *Carpenter*, and the settling point is not clear.").

160. Carpenter v. United States, 138 S. Ct. 2206, 2223 (2018) ("In light of the deeply revealing nature of CSLI, its depth, breadth, and comprehensive reach, and the inescapable and automatic nature of its collection, the fact that such information is gathered by a third party does not make it any less deserving of Fourth Amendment protection.").

161. Rotenberg, *supra* note 159, at 237 (explaining that the lack of clarity provided by *Carpenter* makes it "likely that *Carpenter II* is in the Court's near future").

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

163. *Id.* (quoting Northwest Airlines, Inc. v. Minnesota, 322 U.S. 292, 300 (1944)).

164. *Id.*

165. *See, e.g.*, Aziz Huq, *No, the Roberts Court Is Not Moderating*, TIME (July 6, 2023, 5:00 AM), https://time.com/6292282/the-supreme-court-remains-profoundly-counter-democratic [https://perma.cc/L6AZ-GAFC] (considering the prospective impacts of recent "narrow" decisions); Jeffrey Toobin, *The Trap in the Supreme Court's "Narrow" Decisions*, NEW YORKER (June 30, 2014),

A trend has emerged from the Roberts Court when it claims to have issued a narrow opinion: The holding serves to slightly open a previously shut door before a subsequent case comes along and blows the door off its hinges.[166] One example of this tactic comes from the Court's decisions in 2009 and 2013 regarding the constitutionality of the Voting Rights Act's preclearance requirements. In the 2009 decision *Northwest Austin Municipal District Number One v. Holder*, the Court agreed to hear a constitutional challenge to the preclearance requirements.[167] However, the Court did not have to reach the constitutional question after it concluded that the petitioner was statutorily exempted from the section they were challenging.[168] Arriving at that conclusion, Roberts penned that "[o]ur usual practice is to avoid the unnecessary resolution of constitutional questions."[169] Despite *Northwest Austin* signaling a looming attack on the Voting Rights Act, the seemingly narrow scope of the holding garnered support from each of the Court's liberal members.[170]

Four years later, the Court revisited the Voting Rights Act in *Shelby County v. Holder*.[171] In *Shelby County*, the Court cited its careful consideration of the Voting Rights Act in *Northwest Austin* and the lack of need to rule on the Act's constitutionality in that case.[172] However, the five-member majority made sure to call back to their "broader concerns about the constitutionality of the Act" that emerged in 2009 when considering *Northwest Austin*.[173] Although it was seemingly inappropriate to rule on the constitutionality of the Voting Rights Act's preclearance requirements in 2009, the Court found the facts of *Shelby County* far more inviting to conclude that part of the preclearance requirement had been unconstitutional at least since the Act's most recent renewal.[174] By overriding the will of Congress in 2013 but not in 2009, it appeared as though *Northwest Austin* did little more than tee up the narrow holding of *Shelby County* for the conservative majority.

https://www.newyorker.com/news/news-desk/the-trap-in-the-supreme-courts-narrow-decisions (on file with the *Iowa Law Review*) (looking back on Roberts Court cases that were said to be narrow but were later widened); Chris Schmidt, Note, *Preparing to Open Up Shop: How the Supreme Court Set the Stage to Prohibit Public-Sector Agency-Shop Provisions in* Harris v. Quinn, 134 S. Ct. 2618 (2014), 94 NEB. L. REV. 477, 508 (2015) (expressing the sentiment that, given previous behavior from the Roberts Court, the narrow holding in *Harris* was likely to expand in the then-coming term).

166. Toobin, *supra* note 165 ("It's generally a two-step process: in confronting a politically charged issue, the court first decides a case in a 'narrow' way, but then uses that decision as a precedent to move in a more dramatic, conservative direction in a subsequent case.").

167. Nw. Austin Mun. Util. Dist. No. One v. Holder, 557 U.S. 193, 196 (2009).

168. *Id.* at 207.

169. *Id.* at 197.

170. Toobin, *supra* note 165 ("Chief Justice Roberts's decision was 'narrow,' and it even drew the votes of the court's more liberal members.").

171. Shelby County v. Holder, 570 U.S. 529, 535 (2013).

172. *Id.* at 540.

173. *Id.* at 557.

174. *Id.*

The effect of this two-step process has been described not as a "return to moderation" as some commentators have described, but instead as a stalling tactic.[175] This stalling tactic has allowed the Court to address a smaller portion of a large problem, only to revisit the large problem "five or ten years" down the road.[176] Upon doing so, the Court enabled itself to cite the earlier case as the precedential authority for ruling on the larger issue.[177] Although this approach has been controversial for its erosion of longstanding precedent, its relevance here is only to show that "narrow" holdings have the potential to be anything but narrow.[178] With this information in mind, Chief Justice Roberts' claim that the *Carpenter* holding is "a narrow one"[179] should have no influence on determining whether its reasoning can be applied to other areas of SCA law at least for the sake of hypotheticals.

D. *APPLYING* CARPENTER *TO EXTRATERRITORIAL WARRANTS*

This Section seeks to answer the central question of this Note: How, if at all, does the *Carpenter* decision affect the issuance of extraterritorial warrants issued pursuant to the SCA? Recall that the SCA allows the government to require certain ISPs to disclose information when called upon by "a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . by a *court of competent jurisdiction*."[180] A court of competent jurisdiction includes any court that "has jurisdiction over the offense being investigated."[181] As the federal circuit courts have unanimously found, this language allows a law enforcement officer to acquire a warrant from their jurisdiction and lawfully use that warrant in a separate jurisdiction that presides over the targeted information.[182] However, Rule 41(b) of the FRCRMP generally requires a warrant to be issued by a judge presiding over a given jurisdiction unless one of the narrow exceptions apply.[183]

Two previously mentioned cases—*Guzman Loera* and *Ackies*—ruled on the extraterritoriality issue after *Carpenter* was decided.[184] Both of these cases acknowledged the Supreme Court's decision on CSLI and the reasonable expectation of privacy, yet both followed the pre-*Carpenter* trend of allowing

175. Huq, *supra* note 165.

176. *Id.*

177. *Id.*

178. *See id.* ("Worse, it is cynical but plausible to note that the Court's new strategy is likely to make big changes to the law less obvious, by spreading them out over time. . . . After all, small steps are less likely to catalyze resistance than large leaps.").

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

180. 18 U.S.C. § 2703(a), (b)(1)(A) (emphasis added).

181. *Id.* § 2711(3)(A)(i).

182. United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022) ("[T]hree circuits have ruled that warrants issued pursuant to the SCA are exempted from the venue limitation of Rule 41(b), and no circuit has ruled to the contrary.").

183. FED. R. CRIM. P. 41(b)(1).

184. *Guzman Loera*, 24 F.4th at 144; United States v. Ackies, 918 F.3d 190, 198 (1st Cir. 2019).

the SCA to trump Rule 41's territoriality requirement.[185] Interesting, however, is the fact that the First and Second Circuits did not arrive at their respective conclusions using the same understanding of *Carpenter*.[186]

The First Circuit's decision in *Ackies* was handed down in 2019, one year after *Carpenter* was decided and three years before the Second Circuit's *Guzman Loera* decision.[187] *Ackies* concerned two SCA-backed extraterritorial warrants issued by a magistrate judge in Maine for cellphones located outside of the State.[188] Carey Ackies argued *inter alia* that Rule 41(b) prevented a magistrate judge in Maine from issuing a valid warrant for information held outside of the State.[189] This was because, at least in the eyes of Ackies, the *Carpenter* decision held that cellphones were a tracking device, which require a separate warrant pursuant to 18 U.S.C. § 3117.[190] As the First Circuit concluded, Ackies "incorrectly read[] *Carpenter*," which only mentions the term "tracking device" once.[191]

The court continued on to explain that Ackies was also wrong because *Carpenter* concerned D orders, not warrants.[192] The First Circuit concluded that "[s]ection 2703 treats warrants and orders differently," but failed to elaborate on why the difference in name compelled a different result from *Carpenter*.[193] Based on that generalized conclusion, the First Circuit advanced to the traditional analysis to determine whether Rule 41(b) or § 2703 applied.[194] As mentioned previously, the First Circuit agreed with its sister circuits and held that "Rule 41(b) . . . does not . . . apply to . . . warrants issued under [the SCA]. The text of § 2703 compels this result."[195] For reasons that will be notable later, the First Circuit failed to mention the third-party doctrine or whether Ackies possessed a reasonable expectation of privacy in the cellphones.[196]

The Second Circuit took an alternative route to conclude that *Carpenter* did not compel a different result from the pre-*Carpenter* extraterritoriality cases. Of particular importance is that *Guzman Loera* was argued before a district court after *Carpenter* had been handed down, making it the only appellate decision to have its entire history decided after the Supreme Court's decision.[197] *Guzman Loera* concerned law enforcement's gathering of data using the

185. *Guzman Loera*, 24 F.4th at 158; *Ackies*, 918 F.3d at 198–201.
186. *Guzman Loera*, 24 F.4th at 158; *Ackies*, 918 F.3d at 198–201.
187. *Ackies*, 918 F.3d at 190.
188. *Id.* at 195.
189. *Id.* at 198.
190. *Id.*
191. *Id.*
192. *Id.*
193. *See id.*
194. *See id.* at 201.
195. *Id.*
196. *See generally id.*
197. *See generally* United States v. Loera, 333 F. Supp. 3d. 172 (E.D.N.Y. 2018), *aff'd sub nom.* United States v. Guzman Loera, 24 F.4th 144 (2d Cir. 2022).

spyware "FlexiSpy," which "collects information without the knowledge of device users."[198] Defendant Joaquín Archivaldo Guzmán Loera (commonly known as "El Chapo") captured data of individuals close to him by using FlexiSpy, which then stored the data in "an Amazon cloud server in the Western District of Washington."[199] Law enforcement later gathered this information through a series of three warrants, one of which was signed by a magistrate judge in the Southern District of New York and executed in Washington.[200]

Predictably, Guzmán Loera argued that the magistrate presiding of the Southern District of New York lacked the ability to issue the warrant for information held in the Western District of Washington.[201] Concurring with the decision made by the district court, the Second Circuit held that Guzmán Loera lacked a "reasonable expectation of privacy after giving access to the [FlexiSpy] data to third parties."[202] The Second Circuit concluded that while "neither the Supreme Court nor this Circuit has determined whether warrants issued pursuant to the SCA are exempted from Rule 41(b)'s geographic restrictions," the three circuits to decide the issue have done so correctly and Rule 41(b) does not apply.[203]

Neither *Ackies* nor *Guzman Loera* acknowledged the potentially broader holding of *Carpenter*, which would afford a reasonable expectation of privacy to materials beyond CSLI. The First Circuit failed to do so because Ackies denied ownership of the cellphones targeted by the search warrants.[204] Seeing as Ackies maintained no ownership interest, he vacated a reasonable expectation of privacy, and the First Circuit found that no reasonable expectation of privacy analysis was warranted.[205] The Second Circuit found no reasonable expectation of privacy on different grounds: by claiming the third-party doctrine made doing so irrelevant.[206] Rather than apply a balancing test between the invasiveness of the technology used in the potential search and the extent to which the individual knowingly disclosed the information to a third party, like *Carpenter* suggests, the Second Circuit cites one sentence from the *Carpenter* opinion and adds three words of its own: "'[A] person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.'

198. *Guzman Loera*, 24 F.4th at 157.
199. *Id.* at 149, 157.
200. *See id.* at 158.
201. *Id.*
202. *Id.*
203. *Id.*
204. *See* United States v. Ackies, 918 F.3d 190, 197 n.3 (1st Cir. 2019).
205. *Id.*
206. United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022) ("In addition, the District Court ruled that even if the Fourth Amendment applied, neither downloading the FlexiSpy data nor searching the FlexiSpy data violated the Fourth Amendment because Guzman had no reasonable expectation of privacy after giving access to the data to third parties such as the CS and co-conspirators.").

Again, we agree."[207] This language comes directly from the Supreme Court's 1979 *Smith* opinion, suggesting that—at least in the eyes of the Second Circuit—*Carpenter* 's promise to be a narrow holding was genuine.[208]

But what if the *Carpenter* decision was not as narrow as the Second Circuit believed it to be? Sitting en banc, the Fourth Circuit determined that a claim alleging a Fourth Amendment violation was likely to succeed when the Baltimore Police Department used aerial surveillance over the city of Baltimore.[209] The Fourth Circuit rested its opinion on the Supreme Court's conclusion in *Carpenter*, focusing on the aerial surveillance's ability to indiscriminately track any member of the public beyond one's expectation while they are in public.[210] In the eyes of the Fourth Circuit, the violation of one's reasonable expectation of privacy by using aerial surveillance ensured that "*Carpenter* applie[d] squarely to this case" despite CSLI not being remotely implicated by the surveillance at hand.[211]

The effect of these cases is straightforward: Violating one's reasonable expectation of privacy creates a Fourth Amendment interest that is safeguarded by requiring law enforcement to secure an adequate warrant.[212] But, in light of *Carpenter* and subsequent opinions that have expanded the Fourth Amendment to certain areas previously within the exclusive jurisdiction of the SCA, are extraterritorial warrants still considered adequate? Or were they only adequate when the material they were concerning was outside of the reach of the Fourth Amendment? There is rationale to support both views.

To support the view that extraterritorial warrants issued pursuant to the SCA are valid even when the information is protected by the Fourth Amendment, attention should be given to the Ninth Circuit's 2023 *Moore* decision.[213] In *Moore*, an Idaho state court issued a warrant for the collection of CSLI data stored outside of the state.[214] Relying on the SCA's "court of competent jurisdiction" language, the Ninth Circuit found that Idaho Criminal Rule 41—which is nearly identical to FRCRMP Rule 41 for the purposes of barring

207. United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2216 (2018)).

208. Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

209. Leaders of a Beautiful Struggle v. Balt. Police Dep't, 2 F.4th 330, 340 (4th Cir. 2021) (en banc).

210. *Id.* at 340–41.

211. *Id.* at 341.

212. *See, e.g.*, United States v. Thorne, 548 F. Supp. 3d 70, 123 (D.D.C. 2021) ("[T]he Fourth Amendment also enshrines the 'cardinal rule that, in seizing goods and articles, law enforcement agents must secure and use search warrants whenever reasonably practicable.'" (quoting Chimel v. California, 395 U.S. 752, 758 (1969))).

213. *See generally* United States v. Moore, No. 22-30009, 2023 WL 6937414 (9th Cir. Oct. 20, 2023).

214. *Id.* at *1.

extraterritorial warrants—did not provide sufficient grounds for excluding the CSLI evidence.[215] Although this memorandum opinion offers little in the way of Fourth Amendment analysis and makes no mention of the *Carpenter* decision, its straightforward conclusion that "law enforcement did not violate Rule 41(a) [of the Idaho Criminal Rules] by serving Moore's CSLI warrant outside of Idaho"[216] strongly suggests that the SCA sufficiently protects an individual's Fourth Amendment interest.

Support for the view that Fourth Amendment protection requires more than a warrant issued pursuant to the SCA is far more attenuated but demonstrates a worst-case scenario worthy of being addressed. Recall that Rule 41 of the FRCRMP serves to protect the Fourth Amendment.[217] For the sake of practitioners, following the procedures outlined by Rule 41 will help in avoiding any concerns over a Fourth Amendment violation.[218] Prior to *Carpenter*, the SCA was given significant leeway because it was largely thought that the subject matter the SCA concerned itself with was outside of the scope of the Fourth Amendment.[219] As such, the procedures described by the SCA were not concerned with complying with the Fourth Amendment; they were concerned with creating protections similar, but not the same, as the Fourth Amendment.[220] Importantly, these procedures were not always as protective as the Fourth Amendment.[221] Although this had been suspected by academics, the *Carpenter* decision confirmed such a suspicion by finding D orders constitutionally insufficient to compel CSLI.[222] This leads to the conclusion

215. *Id.* ("Because the Idaho state court qualifies as 'a court of competent jurisdiction,' and because '[Rule 41(a)] was amended to expressly authorize warrants for property located outside the territorial boundaries of the state,' Idaho's 'State warrant procedures' permit extraterritorial CSLI warrants under the SCA. Therefore, law enforcement did not violate Rule 41(a) by serving Moore's CSLI warrant outside of Idaho." (alteration in original) (citations omitted) (first quoting 18 U.S.C. § 2711(3)(B); and then quoting State v. Branigh, 313 P.3d 732, 740 (Idaho 2013))).

216. *Id.*

217. Jones v. United States, 357 U.S. 493, 498 (1958) ("The decisions of this Court have time and again underscored the essential purpose of the Fourth Amendment to shield the citizen from unwarranted intrusions into his privacy. This purpose is realized by Rule 41 . . . which implements the Fourth Amendment . . . ." (citations omitted)).

218. *See, e.g.*, United States v. Horton, 863 F.3d 1041, 1048 (8th Cir. 2017) (demonstrating that, but for the Rule 41 violation, the analysis as to whether a Fourth Amendment violation occurred would not have proceeded).

219. *See* BALSER, *supra* note 36, at 2; Kerr, *supra* note 41, at 1025; *see, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2226 (2018) (Kennedy, J., dissenting) (indicating that each "Court of Appeals to have considered the question" of whether CSLI is protected under the Fourth Amendment has held against applying the constitutional protection).

220. *See* BALSER, *supra* note 36, at 2.

221. Kerr, *supra* note 41, at 1008 ("The federal statute that permits the government to compel contents with less process than a warrant in some cases is therefore unconstitutional in many applications.").

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

that, at least in some circumstances, the Fourth Amendment requires more protection than what the SCA prescribes.

Now knowing that the SCA is, at least on occasion, insufficient to protect Fourth Amendment interests, practitioners are faced with gathering warrants either in accordance with Rule 41 or the SCA. If a practitioner opts to follow the SCA and get an extraterritorial warrant, they are choosing to follow the text of an outdated statute that is known to be at odds with Rule 41, the rule designed to safeguard the Fourth Amendment. This should raise some doubt in the minds of law enforcement, as the potential is there for a court to find the extraterritorial warrant unconstitutional.

The chances of such a result are not impossible, though the immediate impacts would likely be sparse. The unanimity between courts of appeals to rule on the extraterritoriality issue holds weight, but the courts of appeals were also unanimous on the constitutionality of D orders prior to the Supreme Court's ruling in *Carpenter*.[223] Assume then that the Supreme Court or a federal appellate court were to rule that extraterritorial warrants under the SCA were unconstitutional. For years after the decision, the impacts would be minimal due to law enforcement's good-faith reliance on the courts of appeals unanimity in holding extraterritorial warrants valid. This phenomenon has been ongoing with CSLI cases in which the information was gathered prior to *Carpenter*.[224] Eventually, however, courts would have to consider whether to exclude evidence gathered by an unconstitutional warrant.[225] At this time, the logical conclusion for law enforcement is to acquire a warrant using the text of Rule 41.

In the event extraterritorial warrants under the SCA were found to be unconstitutional and warrants had to be acquired from within the jurisdiction that houses the targeted information, judicial economy within those jurisdictions would be stretched beyond a sustainable point. For example, Google currently houses seventeen data centers in the United States and has twelve additional

223. *See* United States v. Guzman Loera, 24 F.4th 144, 158 (2d Cir. 2022) ("[T]hree circuits have ruled that warrants issued pursuant to the SCA are exempted from the venue limitation of Rule 41(b), and no circuit has ruled to the contrary."); *Carpenter*, 138 S. Ct. at 2226 (Kennedy, J., dissenting) (indicating that each "Court of Appeals to have considered the question" of whether CSLI is protected under the Fourth Amendment has held against applying the constitutional protection).

224. *See, e.g.*, United States v. Taylor, 54 F.4th 795, 804 (4th Cir. 2022) ("Even assuming that repoll data is subject to the greater protection of a court-approved warrant, the Government lawfully obtained the information at issue here in good faith reliance on pre-*Graham I* court orders and subpoenas issued in accordance with the SCA."); United States v. Felder, 993 F.3d 57, 77 (2d Cir. 2021) ("In sum, on the facts of this case, the district court did not err in relying on the good-faith exception to the exclusionary rule in admitting historical cell-site location information obtained through a judicial order issued under the Stored Communications Act rather than a warrant supported by probable cause.").

225. *See, e.g.*, *Felder*, 993 F.3d at 75 ("As the Supreme Court has instructed, the exclusionary rule must be the judiciary's 'last resort, not [its] first impulse' when evidence has been procured in violation of the Fourth Amendment. The exclusionary rule serves 'to deter future Fourth Amendment violations,' and thus, the harsh remedy of suppression is warranted 'only where it results in appreciable deterrence.'" (alteration in original) (citations omitted)).

data centers in development.[226] Assuming each of the currently existing data centers is in a separate jurisdiction, that would leave seventeen jurisdictions to handle the entire brunt of Google's search warrant requests. Even without assigning numbers, that is a frightening proposition. When numbers are assigned, it is almost incomprehensible. From July 2023 to December 2023, Google received 35,545 search warrant requests.[227] If those warrant requests were uniformly distributed across the seventeen jurisdictions holding information, that would account for 2,090 requests per jurisdiction. Breaking that number down further, Google alone would require—per jurisdiction—348 search warrant requests per month, 80 per week, or 11 per day. Of course, this number is representative of all search warrants Google was served with. The number is not broken down by state or federal warrants, and it is not broken down by those requested through the SCA. However, these numbers also do not account for any other ISP such as Meta—parent company of Facebook, WhatsApp, and Instagram—or Amazon, which, over the same six-month period as Google, fielded 35,468 and 4,399 search warrant requests respectively.[228]

The chances of *Carpenter* having a meaningful impact on the issuance of extraterritorial warrants are slim. Although the Supreme Court's ruling did open the door for new surveillance technologies to be classified as a breach of one's reasonable expectation of privacy, courts deciding on CSLI data post-*Carpenter* have found that the SCA sufficiently protects that interest despite being at odds with Rule 41(b). However, this does not mean that the conflict between Rule 41(b) and the SCA has been resolved. As evidenced by the Ninth Circuit's recent decision in *Moore*, these issues continue to present themselves and offer courts the opportunity to find that extraterritorial warrants are invalid. As long as the SCA continues to be at odds with the FRCRMP, there is no reason for defense attorneys to cease their attack on extraterritorial warrants. Should one of those novel approaches be persuasive enough to find the SCA's extraterritoriality invalid, a territoriality requirement would be costly for the judicial economy of select jurisdictions. Fortunately, a relatively straightforward solution is available.

226. *Discover Our Data Center Locations*, GOOGLE DATA CTRS., https://www.google.com/about/datacenters/locations [https://perma.cc/5APT-BN8H].

227. *Global Requests for User Information*, GOOGLE TRANSPARENCY REPORT, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=series:requests,accounts;authority:US;time:&lu=user_requests_report_period [https://perma.cc/8PMZ-HWET].

228. *Government Requests for User Data*, META, https://transparency.meta.com/reports/government-data-requests/country/US [https://perma.cc/7JSU-G2AL]; *Law Enforcement Information Requests*, AMAZON, https://www.amazon.com/gp/help/customer/display.html?nodeId=GYSDRGWQ2C2CRYEF [https://perma.cc/C75E-G8M5].

III. IF YOU CAN'T BEAT 'EM, JOIN 'EM: AMENDING THE RULES TO CONFORM TO THE SCA

Despite the confusion regarding the conflict between the FRCRMP and the SCA, Rule 41(b) is not unfamiliar with extraterritorial warrants, nor is Rule 41 unfamiliar with warrants requesting electronically stored information.[229] However, the intersection between the two is sparse.[230] Rule 41(b)(6) allows a magistrate judge to issue a warrant for electronically stored information located "within or outside" of their jurisdiction under two narrow circumstances:

> the district where the media or information is located has been concealed through technological means; or
>
> in an investigation of a violation of 18 U.S.C. § 1030(a)(5), the media are protected computers that have been damaged without authorization and are located in five or more districts.[231]

If law enforcement cannot satisfy those standards, the Rules dictate that a magistrate judge within the jurisdiction of the property being searched must issue the warrant seeking electronically stored information.[232] The lack of congruity with the SCA has resulted—and will continue to result—in litigation if left unresolved.[233]

The simplest solution to the problem addressed in this Note is to eliminate the incongruity between the SCA and Rule 41(b). To do this, Rule 41(b)(6) should be amended to create Rule 41(b)(6)(C), which would allow for the issuance of extraterritorial warrants so long as the investigation is pursuant to § 2703.

A. *AMENDING THE FEDERAL RULES OF CRIMINAL PROCEDURE*

To eliminate this incongruity, the amendment would have to comply with the amendment process for the FRCRMP. The modern process for amending the FRCRMP "is elaborate and time consuming, involving several lawyers of

229. *See* FED. R. CRIM. P. 41(b)(2)–(6) (permitting extraterritorial warrants when a person or property might move outside of the district before the warrant is executed, when the activities related to the warrant pertain to domestic or international terrorism, when law enforcement seeks to use a tracking device, when the warrant relates to a crime in a diplomatic or consular mission in a foreign state, and when electronic information is requested but the location of the information is concealed or it pertains to a violation of § 10300(a)(5) respectively); *id.*(e)(2)(B) ("A warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information.").

230. *Id.*(b)(6)(A)–(B).

231. *Id.*

232. *Id.*(b)(1) ("[A] magistrate judge with authority in the district—or if none is reasonably available, a judge of a state court of record in the district—has authority to issue a warrant to search for and seize a person or property located within the district . . . .").

233. *See, e.g.*, United States v. Moore, No. 22-30009, 2023 WL 6937414, at *1 (9th Cir. Oct. 20, 2023) (showing that litigation regarding extraterritoriality will continue to be filed following *Carpenter*).

review."[234] The amendment process begins with a suggestion that is then reviewed by the Advisory Committee Reporter.[235] The Reporter reviews the submission before sending it to the Advisory Committee.[236] The Advisory Committee has the authority to accept or reject the suggested change outright or make modifications if it sees fit.[237] If the Advisory Committee approves of the suggested change, it is the responsibility of the Reporter to draft the proposed amendment.[238]

The draft then travels to the Standing Committee, where it will undergo scrutiny before being published for public comment.[239] After the period of public comment has expired, the Standing Committee reviews the proposal in light of the public's feedback.[240] If the Standing Committee is satisfied with the proposal after this second round of scrutiny, the proposal will be considered by the Judicial Conference.[241] The Judicial Conference is the final hurdle for the proposal before it arrives at the Supreme Court.[242]

The Judicial Conference is particularly important to the rulemaking process because, while technically involved, the Supreme Court "often . . . approves the proposal as written."[243] With Supreme Court approval, the proposal moves to Congress.[244] By statutory obligation, proposals follow a strict timetable, arriving at Congress by May 1 to allow for a seven-month review period: If no action is taken by Congress, the rules "take effect as a matter of law on December 1 of that same year."[245] Barring a pressing need, the period from proposal to implementation "often takes two [to] three years."[246]

B. Recent Amendments to Rule 41

An amendment to Rule 41 is not out of the realm of possibility. To keep up with the constantly evolving world of surveillance, Rule 41 has been amended seven times in the twenty-first century.[247] Some of these amendments were spurred by legislative action, while others were responding to concerns of the legal community.[248] For example, the Patriot Act of 2001 created Rule 41(b)(3),

234. 1 WRIGHT & LEIPOLD, *supra* note 62, § 2.
235. *Id.*
236. *Id.*
237. *Id.*
238. *Id.*
239. *Id.*
240. *Id.*
241. *Id.*
242. *Id.*
243. *Id.* at 6.
244. *Id.*
245. *Id.*
246. *Id.* at 7.
247. *See* FED. R. CRIM. P. 41 (amended 2001, 2002, 2006, 2008, 2009, 2011, 2016).
248. 3A CHARLES ALAN WRIGHT & SARAH N. WELLING, FEDERAL PRACTICE AND PROCEDURE: FEDERAL RULES OF CRIMINAL PROCEDURE 35 n.12 (4th ed. 2010).

allowing law enforcement to acquire an extraterritorial warrant when it pertained to matters of domestic or international terrorism.[249] Alternatively, Rule 41(b)(4)—allowing magistrate judges to issue extraterritorial warrants pertaining to tracking devices—was added in 2006 in response to concerns about the lack of guidance "for those judicial officers who are asked to issue tracking device warrants."[250] The promulgation of Rule 41(b)(4) is particularly relevant to the discussion of SCA-backed extraterritorial warrants because searches resulting from the use of tracking devices outside of the jurisdiction the warrant was issued was authorized by statute and by two Supreme Court cases, yet it was still added to the Rules.[251]

On December 1, 2016, the most recent amendments to Rule 41 went into effect, creating Rule 41(b)(6).[252] As mentioned above, Rule 41(b)(6) creates two additional exceptions to the general rule of territoriality required by Rule 41(b)(1).[253] Rule 41(b)(6)(B), the second of these two exceptions, allows for an extraterritorial warrant when "the investigation is based on § 1030(a)(5) of the Computer Fraud and Abuse Act."[254] Rule 41(b)(6)(B) will serve as the template for creating a new rule that brings the FRCRMP in line with the powers granted to judges under the SCA.

In the status quo, the litany of litigation has done little to cease lawsuits draining the judicial system of its finite number of resources. The inconsistency between the FRCRMP and the SCA has served as the basis of litigation for more than a decade and a half. Despite definitive rulings from the First, Second, Third, and Seventh Circuits, this issue will still be a matter of first impression for the remaining appellate courts. For the sake of preserving judicial economy and preventing a circuit from barring extraterritorial warrants, Rule 41(b) should be amended to allow for extraterritorial warrants pursuant to the SCA.

CONCLUSION

The incongruity between the SCA and Rule 41(b) has been the source of litigation for nearly two decades. This conflict was easy to resolve under the third-party doctrine, which supported the judicial system's unanimous conclusion that the Fourth Amendment did not apply to the material implicated by the SCA. However, *Carpenter* established that, at least in certain circumstances, material covered by the SCA and the third-party doctrine can still be protected by the Fourth Amendment. Unfortunately, a lack of specificity has left scholars and practitioners guessing as to what the true reach of *Carpenter* is.

249. *Id.*

250. *Id.* at 36 n.13.

251. *Id.* (citing United States v. Karo, 468 U.S. 705, 721 (1984); United States v. Knotts, 460 U.S. 276, 285 (1983); 18 U.S.C. § 3117).

252. *Id.* at 5 n.17 (Supp. 2025).

253. *Id.*

254. *Id.*

For the sake of extraterritorial warrants, courts currently still find the procedures of the SCA sufficient for protecting an individual's Fourth Amendment rights. But will that conclusion continue to be upheld in light of expanding privacy interests in the digital sphere? The SCA has been found unconstitutional in other regards, and as long as it remains at odds with the FRCRMP, litigants will continue to have opportunities to argue that extraterritorial warrants are invalid. If a federal circuit court were to find an extraterritorial warrant invalid, it would have drastic implications for the judicial economy of a handful of jurisdictions.

The conflict between the SCA and the FRCRMP can be resolved by amending Rule 41(b)(6). Currently, Rule 41(b)(6) allows for extraterritorial warrants concerning electronically stored information but only if the warrant satisfies one of two narrow qualifiers. This Note is in support of creating a third qualifier similar to that of Rule 41(b)(6)(2), a qualifier that would allow for extraterritorial warrants when they are issued pursuant to § 2703 of the SCA. Doing so would provide a concrete basis for courts to dismiss claims concerning the validity of warrants issued pursuant to the SCA. By reaching this conclusion, the dispute between the SCA and Rule 41(b) of the FRCRMP can finally be resolved.