Extraterritorial Application of the Stored Communications Act: Why *Microsoft Corp. v. United States* Signals That Technology Has Surpassed the Law

*Adam Gillaspie**

I. INTRODUCTION

In the time that it takes you to read this sentence, more than 11 million new emails will have been sent worldwide.[1] Email is just one of the many forms of electronic communication in the 21st century. The advent of the Internet transformed our society and enabled a world of hyper-connectivity and instant communication with each other, as well as seemingly limitless access to information. The often-ignored reality of technological advances in electronic communication is that with each new development comes the increased potential for an invasion of privacy. Before the telegraph, the only way to intercept communication between individuals meant overhearing a conversation or somehow obtaining a physical letter.[2] Then, it became possible to intercept the electrical signals sent by a telegraph to decipher the electronic communication.[3] Later, with the invention of the telephone came more advanced wiretapping, specifically the ability to listen to conversations without any physical presence at either end of the conversation.[4] Now with the popularity of

* J.D. Candidate, 2018, University of Kansas School of Law; B.S.B. Marketing, University of Kansas, 2015. I would like to thank Beth Hanus, Nathaniel Mannebach, and Professor Jean Phillips for their helpful insight and invaluable comments on this Note, and all of the Staff Members and Editorial Board of the Kansas Law Review for their rigorous and in-depth editing and suggestions. Lastly, thank you to all of my friends and family members for supporting me over the years.

1. An estimated 205.6 billion emails were sent and received per day in 2015, an expected 215.6 billion emails in 2016. THE RADICATI GROUP, INC., EMAIL STATISTICS REPORT, 2015-2019 4 (2015), http://www.radicati.com/wp/wp-content/uploads/2015/02/Email-Statistics-Report-2015-2019-Executive-Summary.pdf.

2. *See generally Ex parte* Jackson, 96 U.S. 727, 733 (1877) (holding that the Fourth Amendment protects sealed letters in the mail).

3. *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 465–66 (1928) (holding that Fourth Amendment does not extend to wiretapping), *overruled in part by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

4. *See, e.g.*, *Katz*, 389 U.S. at 352–53 (noting that the Fourth Amendment can protect oral statements overheard without any technical trespass). *But see* Smith v. Maryland, 442 U.S. 735, 743–

email, text messaging, and other forms of internet communication, it is possible to intercept and easily create a comprehensive account of a person's conversations. By combining the content (e.g. the actual words spoken or written) of the communications themselves and the supporting non-content information—including, among other things, the time, length, and identities of sender and receiver—a much more accurate record of an individual's communications can be compiled than previously possible.[5]

One remarkable aspect of these advances in electronic communications is how little control average consumers have over their emails, text messages, and phone conversations. Once an email or text message is sent, or a phone call made, the relevant service provider obtains certain data about that communication. In the short term, for example, sending a text message creates a record that contains the content of the message, the numbers of both parties, and the date and time of the message.[6] This data will then be stored somewhere on a server owned by the service provider, a decision that is entirely unregulated by any governing body.[7] Usually it is a purely business-minded decision. Microsoft, for example, initially stores customer emails and communications data from the popular Outlook.com email service at the closest datacenter to the location provided during the initial subscription of a particular customer.[8] Later, Microsoft transfers the data to a different datacenter according to the location the user provided when they initially

---

44 (1979) (holding that Fourth Amendment does not apply to pen registers because there is no reasonable expectation of privacy in information voluntarily given to a third party).

5. *See, e.g.*, United States v. Forrester, 512 F.3d 500, 510–11 (9th Cir. 2008) (holding that email headers and IP addresses are akin to pen registers and have no Fourth Amendment protection). *But see* United States v. Warshak, 631 F.3d 266, 282 (6th Cir. 2010) (concluding that an ISP cannot be compelled to turn over the contents of a subscriber's emails because doing so would violate the subscriber's reasonable expectation of privacy under the Fourth Amendment).

6. *See* Joseph B. Evans, *Cell Phone Forensics: Powerful Tools Wielded by Federal Investigators*, FORDHAM J. CORP. & FIN. L.: JCFL BLOG (June 2, 2016), https://news.law.fordham.edu/jcfl/2016/06/02/cell-phone-forensics-powerful-tools-wielded-by-federal-investigators/. Notably, there is no current law in place that requires wireless carriers to store the content of text messages, so none of the major carriers store this portion of the record long-term. *See id.* (explaining that most carriers will delete the contents of text messages "after delivering them" but will retain the transactional data for "sixty days to seven years").

7. While there are statutes regulating electronic communications, discussed *infra*, these laws do not seek to control the physical location of servers because the internet spans across borders. Nonetheless, our data privacy laws resemble a "patch-work quilt," in that regulations are implemented on an industry-by-industry basis and different forms of data are subject to vastly different regulations. *See* Lisa J. Sotto & Aaron P. Simpson, *United States*, *in* DATA PROTECTION & PRIVACY 208–14 (Rosemary P. Jay ed., 2015), https://www.huntonprivacyblog.com/wp-content/uploads/sites/18/2011/04/DDP2015_United_States.pdf.

8. Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 202 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

signed up for Outlook, but ultimately Microsoft has full discretion to control where the data is located at any given time.[9]

Sometimes this results in U.S.-based customers' emails and other relevant data being stored in a separate state, but still within the jurisdiction of the U.S. government. But more often the service providers move the data to servers located in foreign countries, where they have installed datacenters to take advantage of favorable tax benefits and other cost savings. These business decisions have the unfortunate effect of potentially bringing the data out of the reach of lawful criminal investigations seeking warrants in U.S. courts. One example is the recent *Microsoft v. United States* case, in which the Second Circuit overturned a lower court's order that Microsoft produce a customer's email data stored in Dublin, Ireland.[10] In another example, Google has attempted to build off-shore data barges that would be outside the jurisdiction of any sovereign nation.[11]

The law's responses to the advance in electronic communications is notable. Only within the last fifty years has Congress brought electronic transmissions within the confines of Fourth Amendment protection, namely through the enactment of the Electronic Communications Privacy Act and the Stored Communications Act.[12] Because the Fourth Amendment's text only covers individuals' "persons, houses, papers, and effects,"[13] the legislature and judiciary initially resisted extending protections beyond this literal language (i.e. when a new technology is developed), but eventually viewed the protections as necessary with the passing of time and increasing societal adoption of new technologies.[14] Recently, the Supreme Court has grappled with the Fourth Amendment's application to the cellphone, and its more clever cousin the

---

9. *See id*. at 203 ("One of Microsoft's datacenters is located in Dublin, Ireland, where it is operated by a wholly owned Microsoft subsidiary. According to Microsoft, when its system automatically determines, 'based on [the user's] country code,' that storage for an e-mail account 'should be migrated to the Dublin datacenter,' it transfers the data associated with the account to that location. Before making the transfer, it does not verify user identity or location; it simply takes the user-provided information at face value, and its systems migrate the data according to company protocol." (citations omitted)).

10. *See id.* at 200–02.

11. *See generally* Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 716–19 (2011) (describing Google's patent application for a water-based data center and its potential to operate outside the jurisdiction of any country's laws).

12. *See infra* Part II.B (discussing Fourth Amendment jurisprudence and enactment of the Electronic Communications Privacy Act and Stored Communications Act).

13. U.S. CONST. amend. IV.

14. *See supra* notes 2–5.

"smartphone."[15] Some commentators argue that *Riley v. California*, in which the Court held that digital information contained in a cellphone could not be searched absent a warrant, should be extended to include other modern "smart" technologies,[16] like smartwatches and fitness tracking devices.[17]

A recent case is representative of the difficulties courts face when interpreting laws that may no longer be sufficient in light of modern changes in technology. In *Microsoft Corp. v. United States*, the Second Circuit Court of Appeals interpreted the Stored Communications Act ("SCA") to conclude that Microsoft did not have to comply with a warrant—issued under Section 2703 of the SCA—to produce emails stored on a server in a foreign country because the statute did not explicitly or implicitly authorize an extraterritorial application.[18] While this interpretation is both legally and textually sound, the Second Circuit's decision is quite troublesome because the district court's reasoning was equally sound. The problem lies with the ambiguity found in Section 2703 of the SCA. Taking this a step further, the SCA as a whole has largely become obsolete over time and if no changes are made the statute will be become inconsistent with evolving Fourth Amendment protections and privacy law doctrines as applied to current and future technologies. This Note argues that warrants issued under the Stored Communications Act ("SCA warrants") should be treated not as traditional search warrants but rather as subpoenas, or possibly a "hybrid" somewhere between the two, at least until Congress updates the SCA to reflect modern technological advances.

Part II.A of this Note provides a background of Fourth Amendment privacy issues arising from searches of digital technologies. Additionally, Part II.B explores the legislative history of the SCA and how interpretations of the statute have changed over time. Part II.C then outlines the facts, procedural history, and rationale behind the holdings of *Microsoft v. United States*. Building upon this background, Part III.A argues that courts should treat SCA warrants in such a way that does not

---

15. *See, e.g.*, Riley v. California, 134 S. Ct. 2473, 2477 (2014) (holding that officers must have a warrant to search digital information on a cellphone seized after an individual's arrest).

16. The difference between a "smart" and "dumb" technology is the "combination of services, trust, and ease of use" that accompany smart devices. *See generally* James Schaefer, *Smart Devices - What Makes Them "Smart"?*, LEVERAGE BLOG, https://www.leverege.com/blogpost/smart-devices-what-makes-them-smart (last visited Oct. 17, 2017).

17. *See, e.g.*, Katharine Saphner, Note, *You Should Be Free to Talk the Talk and Walk the Walk: Applying* Riley v. California *to Smart Activity Trackers*, 100 MINN. L. REV. 1689, 1692 (2016).

18. Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 200–01 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017); *see also infra* Part II.C (discussing *Microsoft v. United States*).

force the court to engage in analysis of extraterritoriality. Further, Part III.B explains some of the policy outcomes that result from either interpretation of the SCA and lays the foundation for Congress to update the outdated statute. Finally, Part III.C offers some suggestions to amend or replace the SCA to address the aforementioned issues, as well as providing a sustainable solution for future technological advances.

II. BACKGROUND

A. Right to Privacy and the Fourth Amendment

Samuel Warren and Louis Brandeis first conceived the idea of an individual's right to privacy in 1890.[19] A full analysis of the right to privacy is beyond the scope of this Note, but to briefly summarize, there are five dominant species of privacy that have emerged over the past century: 1) tort privacy, 2) Fourth Amendment privacy, 3) First Amendment privacy, 4) fundamental-decision privacy,[20] and 5) State constitutional privacy.[21] Since just before the beginning of the Twenty-First Century, privacy in each of these five forms has been a focal point of many different hot-button issues in American law,[22] including abortion,[23] the right-to-die,[24] drug testing in the workplace,[25] homosexuality,[26] and drunk-driving roadblocks.[27] There have been numerous federal statutes enacted to protect privacy in many areas.[28] Needless to say, privacy is fundamental to American law in many ways.

---

19. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890) ("Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society.").

20. Fundamental-decision privacy involves those fundamental personal decisions that are protected by the Due Process Clause of the Fourteenth Amendment. *See* Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1340, 1391–1420 (discussing fundamental-decision privacy).

21. *See generally id.* (discussing history of privacy in American law).

22. *Id.* at 1342 ("[A]ll of these issues central to our society involve . . . an investigation of the legal concept of privacy, as that term has gained variegated meaning by the year 1992.").

23. *E.g.*, Planned Parenthood of Se. Pa. v. Casey, 505 U.S. 833 (1992) (fundamental-decision privacy).

24. *E.g.*, Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261 (1990) (fundamental-decision privacy).

25. *E.g.*, Chandler v. Miller, 520 U.S. 305 (1997) (Fourth Amendment privacy).

26. *E.g.*, Obergefell v. Hodges, 135 S. Ct. 2584 (2015) (fundamental-decision privacy); Lawrence v. Texas, 539 U.S. 558 (2003) (same).

27. *E.g.*, Mich. Dep't of State Police v. Sitz, 496 U.S. 444 (1990) (Fourth Amendment and state constitutional privacy).

28. For a fairly concise summary of privacy-focused law, including federal and state statutes, U.S. and state constitutional protections, and international privacy protections, *see* DANIEL J. SOLOVE

According to some commentators, the Fourth Amendment is likely the most fundamental form of privacy protection in American law.[29] The Fourth Amendment provides:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[30]

For most of the early history of the United States, the Court considered the Fourth Amendment a property right that prevented the government from unlawfully entering someone's home or taking possession of their tangible property.[31] The Supreme Court, however, significantly expanded Fourth Amendment protections over time to include areas outside the home and to accommodate technological changes in society.

First, in *Olmstead v. United States*, the Supreme Court held that wiretapping of telephone lines was not a violation of the Fourth Amendment because no "search" or "seizure" had taken place.[32] Justice Brandeis, aware of the privacy concerns that accompanied changes in technology, wrote a dissenting opinion that echoed his previous beliefs about the right to privacy.[33] Forty years later, the Supreme Court overruled *Olmstead* and extended Fourth Amendment rights beyond property interests in *Katz v. United States*.[34] There, the Court established the

---

& PAUL M. SCHWARTZ, PRIVACY LAW FUNDAMENTALS (2015).

29. *See, e.g.*, Gormley, *supra* note 20, at 1357–74 (discussing Fourth Amendment privacy throughout the history of American jurisprudence).

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

31. The prohibition against "unreasonable searches and seizures" grew from the strong, property-minded principle that a "man's house is his castle." *See* Gormley, *supra* note 20, at 1358–59. Later, *Boyd v. United States* was the first time the Supreme Court concluded that the Fourth Amendment protection against unreasonable searches and seizures by the government was akin to a privacy right. *See* Gormley, *supra* note 20, at 1359 (citing Boyd v. United States, 116 U.S. 616, 625–26 (1886)).

32. 277 U.S. 438, 466 (1928) ("Neither the cases we have cited nor any of the many federal decisions brought to our attention hold the Fourth Amendment to have been violated as against a defendant, unless there has been an official search and seizure of his person or such a seizure of his papers or his tangible material effects or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure."), *overruled by* Katz v. United States, 389 U.S. 347 (1967), *and* Berger v. New York, 388 U.S. 41 (1967).

33. *Id.* at 473 (Brandeis, J., dissenting) ("Subtler and more far-reaching means of invading privacy have become available to the government. Discovery and invention have made it possible for the government . . . to obtain disclosure in court of what is whispered in the closet."); *see also* Warren & Brandeis, *supra* note 19.

34. *See* 389 U.S. 347, 351, 353 (1967).

"reasonable expectation of privacy" test in applying the Fourth Amendment.[35]

In *Katz*, the government introduced evidence of a telephone conversation that the FBI had obtained via an electronic recording device placed on a public, glass telephone booth.[36] The Court's prior decisions focusing on physical trespass failed to recognize and properly account for advances in technology, a factor implicit in its holding that such surveillance (wiretapping a public telephone booth) was not permissible under the Fourth Amendment.[37] The Court rejected the government's visibility argument, distinguishing between "the intruding eye" and "the uninvited ear."[38] Further, the Court concluded, in accordance with the Fourth Amendment, that "[w]herever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures."[39]

Some years later, the Supreme Court narrowed the scope of what constitutes an unreasonable search and seizure when it determined that individuals have no reasonable expectation of privacy in information voluntarily disclosed to third parties.[40] This rule became known in Fourth Amendment law as the "third-party doctrine."[41] Legal scholars have widely criticized the third-party doctrine since its inception, and some state courts have even outright rejected it under the equivalent state constitutional provisions, yet the doctrine remains valid law.[42] There are

---

35. *Id*. at 360–61 (Harlan, J., concurring).

36. *Id.* at 348, 352.

37. *See id.* at 353, 357–59 ("The Government's activities in electronically listening to and recording the petitioner's words violated the privacy upon which he justifiably relied while using the telephone booth and thus constituted a 'search and seizure' within the meaning of the Fourth Amendment.").

38. *Id.* at 352. The Court reasoned that Katz did not shed his privacy rights "simply because he made his calls from a place where he might be seen," but in fact took affirmative steps (shutting the door of the phone booth) to prevent others from hearing his phone conversations and keep them private. *See id.*

39. *Id.* at 359; *see also id.* at 351 ("[T]he Fourth Amendment protects people, not places.").

40. *See* United States v. Miller, 425 U.S. 435, 442–43 (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 . . . ."); Couch v. United States, 409 U.S. 322, 335–36 (1973) ("[T]here can be little expectation of privacy where records are handed to an accountant, knowing that mandatory disclosure of much of the information therein is required in an income tax return.").

41. *See, e.g.*, Monu Bedi, *Facebook and Interpersonal Privacy: Why the Third Party Doctrine Should Not Apply*, 54 B.C. L. REV. 1, 2 (2013) ("Dubbed the Third Party Doctrine, it states that a person loses Fourth Amendment protection—i.e., does not have a reasonable expectation of privacy—to any communications that the person voluntary discloses to another.").

42. *See, e.g.*, Orin S. Kerr, *The Case for the Third-Party Doctrine*, 107 MICH. L. REV. 561, 563–64 (2009) [hereinafter Kerr, *Case for Third-Party Doctrine*] (stating that the third-party doctrine is "the Fourth Amendment rule scholars love to hate. It is the Lochner of search and seizure law," but providing a defense of the doctrine) (footnote omitted); *see also id.* at 563 n.5 (citing major criticisms

some exceptions to the third-party doctrine, developed both within the judiciary[43] and through federal legislation.[44] The judicial exceptions to the third-party doctrine consist of areas outside the scope of the Fourth Amendment and that are already addressed in other bodies of law that deter governmental abuse of the use of secret agents.[45] Legislation has typically been enacted in response to specific cases. For example, to prevent the use of pen registers without a warrant, Congress enacted the Pen Register and Trap and Trace Devices Statute[46] after *Smith v. Maryland*, in which the Court held their warrantless use permissible under the Fourth Amendment.[47] Other federal statutes include the Electronic Communications Privacy Act ("ECPA"),[48] the Right to Financial Privacy Act ("RFPA"),[49] the Cable Act,[50] and the Video Privacy Protection Act.[51]

B. The Electronic Communications Privacy Act and Stored Communications Act

The relevant exception in this Note is the ECPA. In 1986, Congress' main goal in enacting the ECPA was to update the nearly twenty-year-old Federal Wiretap Act to cover newer communication technologies, namely computer-based communications and other forms of digital communication.[52] The ECPA consists of three parts[53]: Title I is the updated Federal Wiretap Act and covers the interception of any wire, oral,

---

of the third-party doctrine); *but see* United States v. Jones, 132 S. Ct. 945, 957 (Sotomayor, J., concurring) ("More fundamentally, it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.").

43. *See* Kerr, *Case for Third-Party Doctrine*, *supra* note 42, at 590–96 (discussing judicially-created alternatives to Fourth Amendment protections).

44. *See id.* at 596–97 (discussing statutory protections in response to *Miller* and the third-party doctrine, including: Pen Register and Trap and Trace Devices Statute, 18 U.S.C. §§ 3121–27 (2012); Right to Financial Privacy Act, 12 U.S.C. §§ 3401–22 (2006); Health Insurance Portability and Accountability Act, 45 C.F.R. § 164 (2007); and the Stored Communications Act, 18 U.S.C. § 2703 (2012)).

45. *Id.* at 591.

46. 18 U.S.C. §§ 3121–27 (2012); Kerr, *Case for Third-Party Doctrine*, *supra* note 42, at 596.

47. 442 U.S. 735, 745–46 (1979).

48. Pub. L. 99-508, 100 Stat. 1848, 1848–73 (1986) (codified as amended in scattered sections of 18 U.S.C.).

49. 12 U.S.C. §§ 3401–22 (2012 & Supp. 2015) (concerning financial records stored by a financial institution).

50. 47 U.S.C. § 551(h) (2012) (concerning cable company records).

51. 18 U.S.C. § 2710 (2012) (concerning the disclosure of video rental or sale records).

52. *See* U.S. Dep't of Justice, Office of Justice Programs, Bureau of Justice Assistance, *Electronic Communications Privacy Act of 1986*, JUSTICE INFORMATION SHARING, https://it.ojp.gov/privacyliberty/authorities/statutes/1285 (last visited Sept. 30, 2017).

53. *See id.* Titles I and III are irrelevant for my purposes and thus outside the scope of this Note, so I will limit my analysis as appropriate.

or electronic communication,[54] Title II is known as the Stored Communications Act ("SCA") which protects content and subscriber records held by a service provider about or from a subscriber,[55] and Title III addresses "pen registers and trap and trace devices."[56]

1. Overview of the Stored Communications Act

The SCA "was enacted to extend to electronic records privacy protections analogous to those provided by the Fourth Amendment."[57] Specifically, the SCA protected electronic communication services and remote computing services, distinctions that accurately reflected the common understandings of how computer networks functioned *at that time* (i.e. in 1986).[58] Generally, service providers are prohibited from disclosing the records provided to them by their subscribers, although the SCA creates several exceptions to the general obligations of non-disclosure.[59] While not directly relevant to the arguments presented in this Note, it is helpful to understand the overall structure of the SCA as enacted. The beginning section of the SCA imposes criminal punishments for unauthorized use of a service provider's facilities used for storage of electronic communication services.[60] Unauthorized use can either be when one "accesses without authorization," or when one "exceeds an authorization to access . . . and thereby obtains, alters, or prevents authorized access to a wire or electronic communication while it is in electronic storage. . . ."[61]

---

54. Pub. L. 99-508, 100 Stat. 1848, 1848–59 (1986); 18 U.S.C. §§ 2510–22 (2012 & Supp. 2015).

55. Pub. L. 99-508, 100 Stat. 1848, 1860–68 (1986); 18 U.S.C. §§ 2701–12 (2012 & Supp. 2015).

56. Pub. L. 99-508, 100 Stat. 1848, 1868–73 (1986); 18 U.S.C. §§ 3121–27 (2012).

57. Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 206 (2d Cir. 2016) (citing Gov't Br. at 29 (citing S. Comm. on Judiciary, Electronic Communications Privacy Act of 1986, S. Rep. No. 99–541, at 5 (1986)), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017); *see also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 382–86 (2014) [hereinafter Kerr, *Next Generation*] (discussion of ECPA).

58. *See Microsoft v. United States*, 829 F.3d at 206 (citing 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, 1213–14 (2004) [hereinafter Kerr, *A User's Guide*]) (noting that electronic communications services and remote computing services were probably more distinguishable at the time of enactment than they are today).

59. *Id.* at 207.

60. *See* 18 U.S.C. § 2701 (2012).

61. *Id.* Although not explicitly defined in the statute, unauthorized use of electronic storage devices or computer equipment can be accomplished by physically entering the facility without authorization or by "hacking" the computer systems to access the facility. *See* Orin S. Kerr,

As noted, the second section of the SCA imposes a duty of non-disclosure of electronic communications and customer records upon service providers with certain limited exceptions.[62] The SCA distinguishes between "contents of a communication" and "customer records."[63] Section 2703 then establishes conditions under which a service provider is required to disclose the contents of stored communications or non-content related customer information.[64] The provisions of Section 2703 address governmental access to service provider records in a "pyramidal structure."[65] First, the government can obtain from a service provider the most basic non-content information, which includes: name, address, telephone connection records (session times and durations), length of service, types of service utilized, telephone numbers and other subscriber numbers or identities, and means or source of payment.[66] This can be done with relative ease: the government *can* obtain a warrant, court order, administrative subpoena, or consent of the customer, but is not required to do so as long as it is seeking only the non-content information.[67] Should the government choose to obtain a court order, it may obtain additional non-content records upon a showing of "specific and articulable facts showing . . . reasonable grounds to believe that the contents . . . or the records . . . are relevant and material to an ongoing criminal investigation."[68]

Content information—the contents of the electronic communication itself (i.e. the message, text, etc.)—may be obtained without notice to the customer by a warrant ("SCA warrant")[69] or with notice by an administrative subpoena or court order.[70] Additional limitations are placed on the obtainability of the content information depending on how recently the user made the communications.[71] The strictest requirements are found

---

Cybercrime's Scope: Interpreting "Access" and "Authorization" in Computer Misuse Statutes, 78 N.Y.U. L. Rev. 1596, 1600 (2003).

62. *See* 18 U.S.C. § 2702(a) (duty of non-disclosure) and (b) (listed exceptions) (2012).

63. *See id.* § 2702(b), (c).

64. *See* 18 U.S.C. § 2703 (2012).

65. Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 207 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

66. § 2703(c)(2).

67. *See id.* § 2703(c).

68. *Id.* § 2703(d).

69. *Id.* § 2703(b)(1)(A) ("Contents of wire or electronic communications [may be obtained] . . . without required notice to the subscriber or customer, if the governmental entity obtains a warrant issued using the procedures described in the Federal Rules of Criminal Procedure . . . .").

70. *Id.* § 2703(b)(1)(B).

71. *See id.* § 2703(a) (noting different protections for electronic storage more than 180 days old

in Section 2703(a), which states that for content records made and stored within the past 180 days the government is required to obtain an SCA warrant.[72] For content records in storage for more than 180 days the provisions of Section 2703(b) apply, and an SCA warrant must only be obtained if the government is not willing to provide notice to the customer.[73]

As with any federal law, courts interpret the provisions of the SCA based on congressional intent, starting with the explicit statutory language.[74] Where the language is clear and unambiguous, the analysis ends and the statute is interpreted based on the plain meaning of the terms used.[75] But where the language is ambiguous, courts turn to the "statutory structure, relevant legislative history, [and] congressional purposes."[76] The structure of the SCA echoes traditional Fourth Amendment privacy protections for physical objects, especially the home, by creating similar protections for digital and electronic communications that have been disclosed to a third-party service provider.[77] Previously, the Constitution placed no disclosure limits on service providers—because of the third-party doctrine—and so the government could obtain any records with a subpoena and no requirement of notice or consent to the customer.[78] In enacting the SCA, Congress brought digital and electronic communications out of the scope of the third-party doctrine by defining methods for governmental access.[79] The legislative history of the SCA can help courts determine congressional intent regarding specific issues, for example the extraterritorial reach of the SCA as discussed later.[80] The congressional purpose is rather clear—the SCA is a privacy-focused law geared towards electronic communications taking place on computer networks and thereby disclosed to third-party service providers.[81]

---

versus 180 days or less).

72. *Id.*

73. *Id.* § 2703(a), (b)(1)(A).

74. *In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 470 (S.D.N.Y. 2014) (quoting Lamie v. U.S. Trustee, 540 U.S. 526, 534 (2004)) ("In construing federal law, the 'starting point in discerning congressional intent is the existing statutory language.'"), *rev'd*, 829 F.3d 197, 207 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

75. Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999).

76. *In re Microsoft*, 15 F. Supp. 3d at 471 (quoting Fla. Power & Light Co. v. Lorion, 470 U.S. 729, 737 (1985)).

77. *Id.* (quoting Kerr, *A User's Guide*, *supra* note 58, at 1209–13).

78. *See* Kerr, *A User's Guide*, *supra* note 58 at 1209–13.

79. *See id.*

80. *See infra* Part II.C (discussing recent interpretation of the extraterritoriality of the SCA).

81. *See* Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account*

2. Application of the SCA as Technology Advances

When Congress enacted the SCA in 1986, electronic communications were still relatively new. Americans did not use email nearly as widely as today, mostly due to the modern prominence of personal computing[82] and the internet.[83] The main purpose in enacting the SCA, as part of the ECPA, was to update previous federal legislation and ensure that new forms of communication would be afforded the same Fourth Amendment privacy protections as more traditional communication methods despite the third-party doctrine.[84] As technology has advanced, courts have applied the ECPA and SCA without issue because the underlying electronic communications methods have remained relatively similar over time. Text messaging, instant messaging, and social media chat programs function much like email, in that the communications and customer information is stored not only by the consumer on their own device, but also in a facility owned by a service provider. As a result, the SCA has been applied to these new forms of communication[85] relatively easily, and so the SCA has not meaningfully changed since 1986.[86]

Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 217 (2d Cir. 2016) ("[T]he relevant provisions of the SCA focus on protecting the privacy of the content of a user's stored electronic communications. Although the SCA also prescribes methods under which the government may obtain access to that content for law enforcement purposes, it does so in the context of a primary emphasis on protecting user content . . . ."), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

82. Although the first personal computer was released in 1965, it cost more than $3,000 at the time and was mostly purchased for use by NASA. *See The Incredible Story of the First PC, from 1965*, PINGDOM (Aug. 28, 2012), http://royal.pingdom.com/2012/08/28/the-first-pc-from-1965/. Nowadays, computers come in many different sizes, shapes, colors, and prices.

83. For an overview of the internet, see *Brief History of the Internet*, INTERNET SOCIETY, http://www.internetsociety.org/internet/what-internet/history-internet/brief-history-internet#History (last visited Sept. 4, 2017).

84. *See supra* notes 40–51 and accompanying text.

85. *See, e.g.*, Quon v. Arch Wireless Operating Co., 529 F.3d 892, 901–03 (9th Cir. 2008) (applying SCA to text-message service provider), *rev'd on other grounds sub nom.* City of Ontario v. Quon, 560 U.S. 746 (2010); Crispin v. Christian Audigier, Inc., 717 F. Supp. 2d 965, 989–91 (C.D. Cal. 2010) (applying SCA to social-networking sites).

86. One relatively modern advance in technology—cloud computing—has sprung forth a debate about the applicability of the SCA. *See generally* Ilana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617 (2011) (arguing that the SCA is not able to adequately protect cloud storage and should be updated to reflect more recent technological advances). In addition, at least two recent bills would have amended the ECPA and SCA. *See* International Communications Privacy Act, H.R. 5323, 114th Cong. (2016) (amending the federal criminal code and allowing governmental entities to require disclosure of communications in the cloud); Email Privacy Act, H.R. 699 114th Cong. (2016) (proposing an amendment to the Electronic Communications Privacy Act of 1986 prohibiting providers of "remote computing service or electronic communication service to the public from knowingly divulging to a governmental entity the contents of any communication that is in electronic storage or otherwise maintained by the provider, subject to exceptions.").

C. The Microsoft Case

Microsoft v. United States commenced when the government sought to obtain records of an email account potentially used in furtherance of narcotics trafficking.[87] Magistrate Judge James Francis of the Southern District of New York issued an SCA warrant to Microsoft to disclose "information associated with a specified web-based e-mail account that is stored at premises owned, maintained, controlled, or operated by Microsoft Corporation."[88] The warrant directed Microsoft to provide:

> a. The contents of all e-mails stored in the account, including copies of e-mails sent from the account;
>
> b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the types of service utilized, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative e-mail addresses provided during registration, methods of connecting, log files, and means and sources of payment (including any credit or bank account number);
>
> c. All records or other information stored by an individual using the account, including address books, contact and buddy lists, pictures, and files;
>
> d. All records pertaining to communications between MSN . . . and any person regarding the account, including contacts with support services and records of actions taken.[89]

Microsoft complied with the warrant in part by providing the relevant non-content information, but it omitted the content information after determining that the content information for the target account had been transferred to its Dublin datacenter.[90] Microsoft moved to quash the warrant, objecting on the grounds that Rule 41 of the Federal Rules of Criminal Procedure generally does not permit warrants for the search and

---

87. *See* Microsoft Corp. v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 200 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

88. *In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 468 (S.D.N.Y. 2014) (internal quotation marks omitted), *rev'd*, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

89. *Id*.

90. *Id*.

seizure of property outside the United States,[91] and that the SCA does not mention an extraterritorial application.[92]

On the issue of extraterritoriality, Judge Francis determined that the words "using the procedures described in the Federal Rules of Criminal Procedure" found in Section 2703(a) were ambiguous.[93] Judge Francis ultimately denied the motion, indicating that while Microsoft's argument was "not inconsistent with the statutory language, [it was] undermined by the structure[94] of the SCA, by its legislative history, and by the practical consequences that would flow from adopting it."[95]

The main rationale for rejecting Microsoft's extraterritoriality argument was that this particular type of warrant was not like a traditional search warrant but more of a "hybrid" between a traditional search warrant and a subpoena.[96] When issued a subpoena, the recipient is required to produce any information requested within its control.[97] The court felt that since Microsoft owned the server located in Dublin, it was within its control and Microsoft was required to produce any documents or information with no regard to actual physical location of the server on which that information was stored.[98] Judge Francis also suggested that any concerns with the extraterritoriality of the SCA "are simply not present here" because:

> [the] SCA Warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are

91. *Id.* at 470; *see also infra* notes 103–04 and accompanying text (discussing Morrison).

92. *See In re Microsoft*, 15 F. Supp. 3d at 470; *see also* 18 U.S.C. § 2703 (2012).

93. *In re Microsoft*, 15 F. Supp. 3d at 470–71 (noting that this language could either mean "that *all* aspects of Rule 41 are incorporated by reference" or that only the "procedural aspects of the application process are to be drawn from Rule 41") (emphasis added).

94. *See supra* Part II.B.1 (discussing structure of SCA).

95. *In re Microsoft*, 15 F. Supp. 3d at 470; *see also infra* Part III.B (discussing policy concerns).

96. *In re Microsoft*, 15 F. Supp. 3d at 471 (explaining that an SCA warrant is "obtained like a search warrant . . . upon a showing of probable cause . . . [but] is executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question").

97. *Id*. at 472 (citing *In re* Marc Rich & Co., A.G., 707 F.2d 663, 667 (2d Cir. 1983); Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147–48 (S.D.N.Y. 2011); *In re* NTL, Inc. Sec. Litig., 244 F.R.D. 179, 195 (S.D.N.Y. 2007); United States v. Chase Manhattan Bank, N.A., 584 F. Supp. 1080, 1085 (S.D.N.Y. 1984)).

98. The court based this determination on the established principle that a subpoena carries an obligation to produce information regardless of its location. *See id.*

> stored. At least in this instance, it places obligations only on [Microsoft] to act within the United States.[99]

Microsoft then appealed the decision.[100]

On appeal, the Second Circuit Court of Appeals reversed and remanded to the district court, instructing the court to quash the warrant.[101] The Second Circuit rejected the approach adopted by Judge Francis to categorize an SCA warrant as a "hybrid" between a traditional search warrant and a subpoena, and instead interpreted the SCA to use "warrant" as a term of art.[102] In considering whether the SCA would apply extraterritorially, the court began its analysis by reviewing the presumption against extraterritoriality outlined in the Supreme Court's decision in *Morrison v. National Australian Bank Ltd*.[103] In *Morrison*, the Court held that laws enacted by Congress are presumed to only apply domestically unless there is a "clear indication of an extraterritorial application."[104] Because the SCA does not include an explicit extraterritorial application, the government conceded this point in *Microsoft*, and the Second Circuit determined that the warrant provisions did not contemplate or permit extraterritorial application on their face.[105]

The court next analyzed whether the challenged application unlawfully applied the particular statute.[106] In doing so, the court determined the "focus" of the SCA was primarily privacy-based due to the statute's plain meaning,[107] its overall framework,[108] and its legislative history.[109] The court also disagreed with the district court's suggestion that the actual physical location of the server did not invoke extraterritoriality concerns, specifically because in order to actually retrieve the information, Microsoft would have to interact with the Dublin

---

99. *In re Microsoft*, 15 F. Supp. 3d at 475–76.

100. Microsoft v. United States (*In re a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*), 829 F.3d 197, 200 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

101. *Id.* at 201–02.

102. *See id.* at 212–15 (discussing the traditional legal meanings of "warrant" and "subpoena").

103. *Id.* at 210 (citing Morrison v. Nat'l Australian Bank Ltd., 561 U.S. 247 (2010)).

104. *Id.* at 210 (internal quotations omitted) (citing *Morrison*, 561 U.S. at 255).

105. *Id.* at 210, 210 n.19 (citing Recording of Oral Arg. at 1:06:40–1:07:00, 1:25:38–1:26:05).

106. *Id.* at 220 (citing *Morrison*, 561 U.S. at 266–67).

107. *Id.* at 217 (discussing the most natural reading of the language as suggesting privacy as a key concern).

108. *Id.* at 218 (discussing how §§ 2701–2703 all protect against intrusion by unauthorized third parties).

109. *Id.* at 219–20 (discussing how Congress's goal was to "erect a set of statutory protections for stored electronic communications" that would comport with the Fourth Amendment protections available elsewhere).

datacenter in some way, whether through its domestic systems using the internet or by physically going to Ireland.[110] The Second Circuit concluded that with the SCA's privacy focus, the execution of the SCA warrant in question would be an unlawful extraterritorial application of the SCA.[111]

Between the district court's decision and the appeal to the Second Circuit, courts in three different cases cited the district court opinion approvingly, granting an SCA warrant for data located on foreign servers.[112] Prior to October 13, 2016, when the Justice Department requested a rehearing en banc of the ruling in *Microsoft v. United States*,[113] only one court had taken a similar position to the Second Circuit's ruling in *Microsoft*, denying extraterritoriality in the Racketeer Influenced and Corrupt Organizations Act.[114]

The Second Circuit ultimately denied the government's request for rehearing on January 24, 2017, after failing to receive a majority of votes favoring en banc review.[115] Nonetheless, five members of the court wrote opinions expressing many of the concerns resulting from the prior decisions by the district court and the Second Circuit.[116] In an opinion concurring in the denial of rehearing en banc, Circuit Judge Susan L. Carney agreed with the panel's reasoning in its majority opinion, but repeatedly referenced the inadequacy of the SCA in the current state of technology.[117] The remaining four opinions were authored by the

---

110. *See id.* at 220 ("Microsoft will necessarily interact with the Dublin datacenter in order to retrieve the information . . . .").

111. *Id.* at 220–21.

112. *See* United States v. Martin, No. CR-14-00678-PHX-DGC, 2015 WL 4463934, at *3–4 (D. Ariz. July 21, 2015) (following the district court approach and concluding that the SCA warrants issued "were not improper exercises of extraterritorial jurisdiction" when used to access data on Facebook and Twitter servers alleged to be located in Germany); United States v. Scully, 108 F. Supp. 3d 59, 77–78, 83 (E.D.N.Y. 2015) (explaining that the SCA language was ambiguous and adopting the approach taken by the district court); *In re* a Warrant for All Content & Other Info. Associated with the Email Account xxxxxxx@Gmail.com Maintained at Premises Controlled by Google, Inc., 33 F. Supp. 3d 386, 389 n.1 (S.D.N.Y. 2014) (quoting Judge Francis's rationale for adopting the hybrid search warrant approach).

113. Petition for Rehearing and Rehearing En Banc at 21, Microsoft Corp. v. United States, 855 F.3d 53 (2d Cir. 2017) (No. 14-2985).

114. *See* Elsevier, Inc. v. Grossman, 199 F. Supp. 3d 768, 781–82 (S.D.N.Y. 2016) (interpreting 18 U.S.C. §§ 1961–68 (2012)).

115. Microsoft Corp. v. United States, 855 F.3d 53, 54 (2d Cir. 2017). With three circuit judges recused from the voting, *id.* at 54 n.*, the panel was split at 4-4, and the rehearing was denied.

116. *Id.* at 54.

117. *See id.* at 55 (Carney, J., concurring) ("We recognize at the same time that in many ways the SCA has been left behind by technology."); *id.* at 59 (Carney, J., concurring) ("Fragmentation, an issue raised by the government in its petition and by the dissents here, was not present in the facts before the panel, and only further emphasizes the need for a modernized statute."); *id.* at 60 (Carney,

dissenters. All of the authoring judges and the parties agreed that the SCA lacks a clear textual basis for extraterritoriality,[118] but each dissenter reiterated as a critical issue of their argument the district court's determination of the irrelevancy of the precise location of the server on which the data was located.[119]

In the wake of the Second Circuit Court of Appeals' denial, the controversy is nowhere near settled. A bonafide circuit split has yet to fully manifest, but courts continue to favorably cite to the Second Circuit decision in *Microsoft*, as well as the district court decision it overruled.[120] Ultimately, this dispute is now on track for final resolution by the Supreme Court.[121] There appears to be significant external support for both sides.[122] The Court must now reach a resolution that creates the best "balance

---

J., concurring) ("And we can expect that a statute designed afresh to address today's data realities would take an approach different from the SCA's, and would be cognizant of the mobility of data and the varying privacy regimes of concerned sovereigns, as well as the potentially conflicting obligations placed on global service providers like Microsoft.").

118. *E.g.*, *id.* at 55 (Carney, J., concurring) ("[I]t is common ground that Congress did not intend for the SCA's warrant procedures to apply extraterritorially."); *id.* at 60 (Jacobs, J., dissenting) ("As all seem to agree, and as the government concedes, the Act lacks extraterritorial reach.").

119. *See id.* at 61 (Jacobs, J., dissenting) ("[N]o extraterritorial reach is needed to require delivery in the United States of the information sought, which is easily accessible in the United States at a computer terminal."); *id.* at 63 (Cabranes, J., dissenting) ("The panel majority ignored the fact that Microsoft lawfully had possession of the emails; that Microsoft had access to the emails in the United States; and that Microsoft's disclosure of the emails to the government would take place in the United States."); *id.* at 70 (Raggi, J., dissenting) ("It is simply unprecedented to conclude that the presumption against extraterritoriality bars United States courts with personal jurisdiction over a United States person from ordering that person to produce property in his possession (wherever located) when the government has made a probable cause showing that the property is evidence of a crime."); *id.* at 76 (Droney, J., dissenting) ("Microsoft has possession and immediate access to those emails regardless of where it chose to store them.").

120. As of September 2017, the District Court decision has been cited eight times, the Second Circuit decision has been cited twenty-three times, and the rehearing denial has been cited fourteen times.

121. The Justice Department's petition for writ of certiorari was granted on October 16, 2017. Microsoft Corp. v. United States, 2017 U.S. LEXIS 6343 (Oct. 16, 2016).

122. *See, e.g.*, Allison Grande, *State AGs Press High Court to Take on Microsoft Warrant Row*, LAW360 (Aug. 2, 2017, 10:48 PM), https://www.law360.com/articles/950796?scroll=1 (describing amicus brief in which state attorneys general ask the Supreme Court to reverse the Second Circuit because its ruling allows "businesses to unfairly dodge an obligation to cooperate in criminal probes"); Peter J. Henning, *Digital Privacy to Come under Supreme Court's Scrutiny*, N.Y. TIMES (July 7, 2017), https://www.nytimes.com/2017/07/10/business/dealbook/digital-privacy-supreme-court.html?mcubz=3 ("Those requests are often granted because the justices rely on the solicitor general's office to identify cases that have significant law enforcement implications."); Sophia Morris, *Google Won't Challenge Warrants For Overseas Data: DOJ*, LAW360 (Sept. 14, 2017, 6:04 PM), https://www.law360.com/articles/964048/google-won-t-challenge-warrants-for-overseas-data-doj; Steven Trader, *Feds Ask Justices To Review Microsoft Overseas Warrant Win*, LAW360 (June 26, 2017, 8:01 PM), https://www.law360.com/articles/938342.

between privacy interests and law enforcement needs in a digital world."[123]

III. ANALYSIS

A. SCA & The Microsoft Case

The SCA inadequately protects the most common forms of electronic communications in modern society. While at one time the SCA applied the Fourth Amendment to electronic communications appropriately, advances in technology mean that the statute is being applied in situations and to forms of electronic communication that the legislature in 1986 could not have predicted. The SCA is narrowly written with an eye towards providing Fourth Amendment-like protections for electronic communications taking place on pre-internet computer networks. With the internet, traditional understandings of international borders are becoming obsolete. On its face, the SCA is unclear as to how far geographically the statute reaches. Because the plain language of Section 2703(a) is unclear regarding extraterritoriality, courts must consider congressional intent based on its overall structure established thirty years ago, a scant legislative history that equally supports two opposing views, and a privacy-focus that has changed substantially over time. While in 1986 the SCA was sufficient to fulfill its intended purpose—granting electronic communications equivalent protection under the Fourth Amendment—it no longer serves that purpose and should be updated to reflect technological changes in the past thirty years and in such a way that contemplates future advances.

1. SCA Warrant as Hybrid Search Warrant?

The district court's decision to categorize an SCA warrant as a "hybrid" between a traditional search warrant and a subpoena aligns with the statutory provisions. The structure of the SCA allows the government the option to obtain an SCA warrant for any information but only *requires* a warrant supported by probable cause for the contents of emails made within the previous 180 days.[124] In other words, in situations where the

123. Allison Grande, *In Microsoft, Justices To Set Feds' Reach For Overseas Data*, LAW360 (Oct. 17, 2017, 2:53 PM), https://www.law360.com/articles/974907/in-microsoft-justices-to-set-feds-reach-for-overseas-data.

124. *See* 18 U.S.C. § 2703(a) (2012) (referring to a warrant issued in conformance with the Federal Rules of Criminal Procedure, which further require probable cause. FED. R. CRIM. P. 41(d)(1)).

government is not required to obtain a warrant, it will not be motivated to do so and will instead probably seek a subpoena, which compels a service provider to provide the records even if they are overseas.[125] Even where an SCA warrant is obtained, there is no functional difference between the SCA warrant and a subpoena for service providers like Microsoft, who will ultimately disclose the information.

More than likely, after being issued a subpoena Microsoft will direct an employee or representative to obtain the non-content records requested therein by accessing the data stored in the Dublin datacenter through the internet from a location in the United States. Alternative methods, like having a Dublin-based employee personally deliver the records to the United States or paying for a U.S.-based employee to retrieve the records from Dublin, would be implausible, cost-inefficient, and needlessly timely. Had Microsoft chosen to comply fully with the SCA warrant, their process for obtaining the relevant data would be the same: a Microsoft employee or representative would have accessed the data through the internet from a physical location within the United States. Even though the SCA does use the term of art "warrant," whether the legislature intended for an SCA warrant to fully mirror traditional search warrants issued under the Fourth Amendment is unclear, as demonstrated by the conflicting opinions issued by the Southern District of New York and the Second Circuit Court of Appeals, as well as many other courts since.[126]

If SCA warrants are treated as hybrid search warrants in the way the district court would have allowed, there will be both legal and practical advantages and disadvantages. The main benefit of this approach is that access to electronic communications records will not be placed completely out of the reach of lawful government investigations by being stored abroad. In order to obtain an SCA warrant, the government must still show probable cause in accordance with the Fourth Amendment and the Federal Rules of Criminal Procedure,[127] but the service provider will not be able to conceal these records by moving them to a server in a foreign country to save money or, in the case of a customer request, by incorrectly telling the service provider he or she is in Dublin.

---

125. *In re* a Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014) ("It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information.") (citing Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983)), *rev'd*, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

126. *See supra* notes 112–14, 120 and accompanying text.

127. *See* 18 U.S.C. § 2703(a) (2012) (incorporating the Federal Rules of Criminal Procedure, including FED. R. CRIM. P. 41).

As at least one commentator has pointed out after the district court's decision, this application of the SCA also offends "international comity."[128] Substantial commentary on this case arose after the district court rendered its decision and focused primarily on the extraterritorial implications of that decision.[129] For a traditional search warrant that relates to searches or seizures made overseas, the government must rely on treaties with foreign nations—mutual legal assistance treaties ("MLATs").[130] The hybrid approach may give the government too much power and allow it to circumvent international laws and the MLAT process to obtain electronic records that are otherwise protected.[131]

2. SCA Warrant as Traditional Search Warrant?

The Second Circuit treated SCA warrants as traditional search warrants, which is an equally sound determination based a plain meaning interpretation of the SCA. However, the ambiguity in the statute and the paucity of legislative history on the matter could be interpreted either way. The legislature could have intended for an SCA warrant to mirror traditional search warrants completely or it could have meant to heighten the requirement to obtain an SCA warrant in procedure alone but still compel the service provider to produce the electronic communication records. The Second Circuit's reasoning ignores the actual method by which service providers will comply with an SCA warrant in these types of situations. The Second Circuit also made a critical determination by deciding that the physical location of the server is highly important. Once this decision was made, a favorable outcome for Microsoft was all but guaranteed because the location of the data on the server in Dublin was undisputed. Unless stated otherwise, a U.S. statute is strongly presumed to not apply extraterritorially.[132] The rest of the court's analysis hinges on this determination.

---

128. Lindsay La Marca, Note, *I Got 99 Problems and a Warrant Is One: How Current Interpretations of the Stored Communications Act Offend International Comity*, 44 HOFSTRA L. REV. 971, 973 (2016).

129. *See, e.g.*, Alexander Dugas Battey Jr., Comment, *A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act*, 42 RUTGERS COMPUTER & TECH. L.J. 262 (2016) (discussing *Morrison*, conflict of international laws, process for mutual legal assistance treaties, and suggesting modernization of data transfer procedures between sovereign nations); La Marca, *supra* note 128, (discussing the SCA, the Fourth Amendment, and the Federal Rules of Criminal Procedure synergy, as well as *Morrison* and mutual legal assistance treaties procedures; then making suggestions for legislative reform).

130. *See* La Marca, *supra* note 128, at 992–93.

131. *Id.*

132. Morrison v. National Australian Bank Ltd., 561 U.S. 247, 248 (2010).

Treating an SCA warrant as a traditional warrant also has advantages and disadvantages. The government's power would be limited to obtaining only those records that are within its jurisdictional control or covered by an MLAT. Concerns with extraterritoriality, or circumventing international laws, are rendered moot. As indicated previously, however, the SCA only requires the government to obtain a warrant for contents of electronic communications made within the previous 180 days. If service providers comply with an SCA warrant in the same way as a subpoena issued for the same or similar records (offset by the temporal limits of the SCA), the practical difference between these two is nearly nonexistent. Just as Microsoft has done, service providers will refuse to produce records requested by SCA warrant. The largest negative effect is that with no access to content records from the previous 180 days stored in a specific location by a service provider, government investigations will be severely hindered because of a business decision by a service provider to save money by locating its servers overseas. Ultimately, the SCA's "warrant" can plausibly be interpreted as a traditional search warrant or a subpoena. Advances in technology and the prevalence of email and other forms of digital communication necessitate an increasing reliance on third-party service providers who are storing that data. This change has revealed an ambiguity in the SCA that was easily overlooked by Congress in 1986, with the SCA no longer sufficiently serving its original purpose.

3. The "Correct" Outcome

Either of the interpretations given throughout the proceedings of *Microsoft* are "correct." Both the district court and the Second Circuit applied the proper statutory interpretation rules, but in the end, they produced entirely different results. Nonetheless, the hybrid approach taken by the district court is a better outcome because the SCA warrants are limited in subject matter in that they are only being issued on service providers to provide records of email and other electronic communications. Congress' attempt to remove these records from the confines of the third-party doctrine has resulted in an incompatible result. An SCA warrant directs service providers to produce the same exact sorts of records as a subpoena, the only difference being how recently the communications may have been sent.

Once one takes into account the technical differences between electronic communications as they occurred in 1986—via individual computer networking and before the internet—versus the methods used for email, text messaging, instant messaging, and other forms of modern electronic communications, the urgency to fix the SCA is apparent. Back

in 1986, any records that would have been subject to the SCA were likely communications between parties in the United States that travelled directly between them and were only stored in two domestic locations—the computer of the sender and the computer of the receiver. Whereas now, an email or text message between the same two parties could travel between numerous locations worldwide, all in the blink of an eye, and ultimately end up "stored" on a data server in Ireland. Also, as noted by one of the dissenters in the denial of the rehearing en banc, some service providers are already undermining the effectiveness of an SCA warrant in light of the Second Circuit's decision by refusing to disclose information stored abroad.[133]

Seeing courts adopt the hybrid approach also invokes a more immediate basis for change by the legislature than continuing to treat an SCA warrant as a traditional search warrant would. Consider the path that most new communications technologies have undergone before eventually being given Fourth Amendment-like protections.[134] Usually when a new technology is created, it is adopted by the public, and eventually the government will find a way to track or reach those communications. Then, those technologies will either be granted Fourth Amendment protections in the form of a judicial decision or by the legislature in the form of a statute.[135] Email, while technically covered under the SCA, is a fairly new form of electronic communication, or at least different enough from the electronic communications that existed in 1986 when the SCA was enacted, to justify new protections. *Microsoft* is an opportunity for the courts and legislature to ensure that new forms of electronic communication are guaranteed the protections they deserve under the Fourth Amendment. Whether that comes in the form of a Supreme Court decision, an amendment to the SCA, or an entirely new statute by the legislature, a change is needed.

---

133. Microsoft Corp. v. United States, 855 F.3d 53, 64–65 (2d Cir. 2017) (Cabranes, J., dissenting) (explaining that Google will now only disclose information already stored in the United States as of the time of the warrant being served and that Yahoo! won't even ensure that data stored abroad is preserved), *cert. granted*, 2017 U.S. LEXIS 6343 (Oct. 16, 2017).

134. *See supra* notes 32–51 and accompanying text (discussing how technological change has historically involved initial reluctance and eventual expansion of the Fourth Amendment).

135. A historical example of this process is the courts' review of law enforcement's wiretapping of public phone booths and telephone lines. *See id.* More recently, Courts have begun to grapple with cellphones. *See* Riley v. California, 134 S. Ct. 2473 (2014) (warrantless search of cell phone in search incident to arrest violated the Fourth Amendment); *but see* United States v. Carpenter, 819 F.3d 880 (6th Cir. 2016) (use of cell phone tower data to track location did not constitute a Fourth Amendment search), *cert. granted sub nom.* Carpenter v. United States, 137 S. Ct. 2211 (2017).

B. Effects & Policy Considerations

Either interpretation—SCA warrant as hybrid search warrant or SCA warrant as a traditional search warrant—raises legitimate policy concerns. Treating an SCA warrant as a traditional search warrant limits the reach of a legitimate government investigation in obtaining electronic communications of suspects or criminal defendants. But since the government in no way regulates the service providers as to data storage and the internet allows transfer of data across the world in an instant, Microsoft and others are free to store these records on any server within their control. The applicability of the SCA should not hinge on a purely business-based decision because this allows private entities to dictate how the law will apply in certain situations.[136]

Consequently, since the data storage policies of service providers like Microsoft are not regulated, they have no incentive to take any extra steps to adhere to federal laws like the SCA in regards to where they store their data for the benefit of the government. Since the records are stored based on customer-provided location information, any individual with nefarious means can successfully conceal electronic communications from governmental access by lying about their actual locations when they sign up for a new service. Even law-abiding individuals who are concerned about their privacy may want to protect their electronic communications from prying government eyes if they know they can avoid it by merely telling their ISP they are from a different country.

C. Updating the SCA

Updating the SCA,[137] and other similarly outdated statutes, to address the issues in *Microsoft Corp.* and to more accurately reflect advances in technology would help courts more accurately address the above issues regarding electronic communications and other data. For instance, the USA PATRIOT Act of 2001 enabled the government to track and intercept nearly all forms of communication by creating new crimes and procedures and making sweeping amendments to many different sections of the Code, all as a powerful response by Congress to the terrorist attacks on 9/11.[138]

---

136. The obvious criminal investigations at stake involve email-based crimes, like fraud in the form of email or phishing scams. However, as the internet continues to be a part of our lives, more and more forms of crime will likely start to cross over into the digital world, e.g. cyber-bullying, internet-initiated sex crimes, et al.

137. *See* Kerr, *Next Generation*, *supra* note 57, at 411–18 (discussing suggestions for updating the entire ECPA).

138. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept

Also, the Federal Rules of Civil Procedure were updated in 2015 with fairly substantial e-discovery amendments.[139] Updating the SCA is not as complex as it may appear at first blush. Electronic communications and other forms of data are nothing more than intangible assets, which courts have been dealing with for much longer than they realize:

> [T]he jurisdictional challenges presented by the global cloud are not conceptually as novel as they seem. Despite the technological wizardry of modern life, the "cloud" is actually a network of storage drives bolted to a particular territory, and there is substantial case law suggesting that courts think of data as a physical object. Moreover, even if the cloud were a free-floating ether, data can be thought of as an intangible asset, like money or debt, which flows across borders; courts have been adjudicating such jurisdictional disputes for centuries. These precedents suggest numerous grounds for states to assert jurisdiction over data—not a single test, as major Internet companies claim.[140]

Some amendments to the SCA have already been proposed. The most recent, the Email Privacy Act, sought to address some of the concerns raised in this Note by changing the usage of "divulge" in some sections to "disclose" and clarifying some procedural requirements.[141] Other proposed amendments have sought to eliminate the 180-day rule.[142]

At a minimum, Congress should amend the SCA to address the extraterritoriality issue. If it chooses to simply include a provision regarding whether the law should apply extraterritorially, that will at least solve one aspect of the dispute between service providers, like Microsoft, and the government. But Congress should not limit itself to applying a band-aid on the current law. Either a complete overhaul or an entirely new statute would be better. A new framework that better serves the government's ability to obtain electronic communications information, as well as individual privacy concerns, will shield courts from criticism after applying an outdated statute to modern technologies. This new version of the SCA should provide guidelines for ISPs on where and how to store their customers' data, as well as a warrant/subpoena procedure for situations where a U.S.-based company has chosen to transfer data to

---

and Obstruct Terrorism (USA PATRIOT ACT) Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (codified as amended in scattered sections of the U.S.C.).

139. *See, e.g.*, FED. R. CIV. P. 26 (2015 amendments).

140. *See* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 729 (2016) (the article more generally discussing treatment of data in the law, making the argument that data is not any different than other intangible assets, and suggesting practical steps that can be taken to address jurisdictional conflicts).

141. Email Privacy Act, H.R. 699, 114th Cong. (2015).

142. Electronic Communications Privacy Act Amendments Act of 2015, H.R. 283, 114th Cong. § 3 (2015).

another country for purely economic reasons.

IV. CONCLUSION

The drafters of the Fourth Amendment recognized the importance of privacy and sought to protect individuals from unreasonable searches and seizures of their property by the government. At first, protections were limited to the home, but eventually were interpreted to include public areas where a person has a reasonable expectation of privacy. Then, the reasonable expectation of privacy afforded in certain contexts was interpreted to exclude information and records voluntarily disclosed to third parties. As technology continued to advance, Congress felt it necessary to protect certain forms of information by granting Fourth Amendment-like protections through statutory frameworks for new types of physical and electronic records.

In the SCA, Congress sought to protect electronic communications disclosed and stored by third-party service providers. The SCA has operated for the past thirty years with relative consistency and has been interpreted to include newer forms of digital communication, like text messaging and social media programs. However, as seen in *Microsoft*, the time has come to update the SCA to clear up the ambiguities that have arisen because of advances in technology. In *Microsoft*, the Second Circuit held that the SCA did not contemplate an extraterritorial application and thus Microsoft did not have to produce emails stored on a server in a foreign country. This decision is the incorrect outcome because an SCA warrant is more like a subpoena, or at least a hybrid between a subpoena and a traditional search warrant.

Going forward, the SCA must be updated to reflect technology changes over the past thirty years and to reflect changes that may appear in the future. Meanwhile, courts should interpret the SCA in a way that treats SCA warrants more like subpoenas, as the district court in *Microsoft* indicated. Doing so is more in line with the structure of the SCA than an alternative approach. Further, this interpretation alleviates any potential circumvention of legitimate criminal investigations where the government would otherwise be shut off from obtaining electronic communications records due to either a business decision made by a service provider or a conscious decision by a customer to conceal their records by providing misleading information to the service provider. As technology continues to improve, courts and the legislature must be constantly vigilant of the existing laws and their continuing applicability. Should the opportunity for individuals to take advantage of gaps in statutory provisions arise, the law should be quick to address these shortcomings.