Hofstra Law Review

Volume 44 | Issue 3 Article 12

3-1-2016

I Got 99 Problems and a Warrant Is One: How Current Interpretations of the Stored Communications Act Offend International Comity

Lindsay La Marca

NOTE

I GOT 99 PROBLEMS AND A WARRANT IS ONE: HOW CURRENT INTERPRETATIONS OF THE STORED COMMUNICATIONS ACT OFFEND INTERNATIONAL COMITY

I. INTRODUCTION

As of 2012, there were 3.3 billion email accounts in the world and that number is expected to increase by six percent each year, amounting to approximately 4.3 billion accounts in 2016.[1] In 2013, there were approximately 7.137 billion people in the world.[2] This implies that approximately half of the people in the world are email account holders.[3] A large number of these emails are stored overseas.[4] For example, Microsoft, just one of the many companies that operate email servers, recently admitted that the data from more than one billion of its customers—including the data for over 20 million businesses—is stored on one-hundred servers in forty countries.[5] This potentially subjects millions of customer email to the overreaching tentacles of the U.S. government without any Fourth Amendment protections.[6]

The Stored Communications Act of 1986 ("SCA")[7] was initially passed by Congress to prevent unlawful government searches and seizures of electronic information held by third parties.[8] Under the SCA, law enforcement agencies may lawfully obtain electronic information

1. THE RADICATI GRP., EMAIL STATISTICS REPORT, 2012-2016, at 2 (Sara Radicati ed., 2012).

2. POPULATION REFERENCE BUREAU, 2013 WORLD POPULATION SHEET 3 (2013).

3. *See id.*; THE RADICATI GRP., *supra* note 1, at 2.

4. *See, e.g.*, Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States at 5-6, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained By Microsoft Corp., 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (No. 13-MJ-2814).

5. *Id.* at 8.

6. *See* U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 351 (1967).

7. 18 U.S.C. §§ 2701–2712 (2012).

8. *See id.*; Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 383 (2014).

held by third parties via three methods: a court order,[9] an administrative subpoena,[10] or a search warrant.[11] Today, many critics argue that the SCA does not adequately protect such communications.[12] In the nearly thirty years since the SCA was enacted, the idea of electronic storage has drastically evolved.[13] Now, Internet service providers ("ISP(s)") are creating "server farms" or "data centers"[14] where massive amounts of electronic data can be stored.[15] More importantly, many of these "farms" are located in other countries.[16] This information may be obtainable by U.S. law enforcement agencies through the use of a Mutual Legal Assistance Treaty ("MLAT"), which assists law enforcement agencies in conducting searches and seizures abroad.[17] Conversely, the information sought may be outside U.S.-jurisdictional reach when there is no MLAT between the United States and the country in where information is stored.[18]

Nevertheless, an opinion recently issued in the Southern District of New York in *In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.* ("*Microsoft Case*") held that the SCA is applicable far beyond U.S. borders and thus may have consequences for many unsuspecting email account holders.[19] The court

---

9. § 2703(b)(1)(B)(ii).

10. § 2703(b)(1)(B)(i).

11. § 2703(b)(1)(A).

12. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233 (2004); Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 382 (2009).

13. *See* Kerr, *supra* note 8, at 390 (discussing the advances in technology that render the current legislation ineffective).

14. One author has explained server farms and data centers as such: "Put simply, a server is a computer designed to provide information or processes to other computers on a network, and a server farm, also known as a data center, is a group of servers in one location connected by a network." Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 714 (2011).

15. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014) [hereinafter *Microsoft Case*] ("[Companies like] Microsoft store[] e-mail messages sent and received by its users in its datacenters.").

16. *See id.*; Kerr, *supra* note 8, at 406.

17. *See MLAT: A Four-Letter Word in Need of Reform*, ACCESSNOW (Jan. 9, 2014, 5:20 PM), https://www.accessnow.org/blog/2014/01/09/mlat-a-four-letter-word-in-need-of-reform (explaining what an MLAT is and how it works). MLATs are treaties between two countries that allow each nation to request help in the executing a search warrant when the subject is within the territory of the other nation. *See id.*

18. *Microsoft Case*, *supra* note 15, at 475 (demonstrating that if a foreign country declines to assist the United States in executing a search warrant, the electronic information will not be accessible).

19. *Id.* at 471, 476.

held that an SCA search warrant compelling Microsoft to produce a customer's emails stored on a server in Ireland was enforceable.[20] This decision is likely to have a considerable impact on ISPs and the American public because ISPs will now be compelled to share information that was previously expected to be protected by the Fourth Amendment.[21] Up to one half of the world's population could be affected by the potential ramifications of the SCA and the potential ability of the U.S. government to reach into the email accounts of users worldwide.[22] This decision has brought to light the jurisdictional problems that the SCA presents in its current form.[23] Moreover, the interpretation of the SCA in this decision may offend well-settled principles regarding transnational law, treaties, and international comity.[24]

This Note addresses some of the issues highlighted above which have yet to be resolved by lawmakers. Part II of this Note describes how the SCA, the Fourth Amendment, and the *Federal Rules of Criminal Procedure* work in conjunction with each other.[25] Additionally, Part II explores Congress's jurisdictional capabilities outside of the United States.[26] Part III then highlights some of the current problems caused by the SCA and the *Microsoft Case*, which recently addressed many of them.[27] Finally, Part IV proposes

20. *Id.* at 467, 471, 477 (stating that a search warrant issued pursuant to 18 U.S.C. § 2703(a) maintains a special status as a hybrid between a subpoena and a search warrant); *see also SDNY Judge Orders Microsoft to Produce Emails Stored Abroad*, BRACEWELL (Aug. 4, 2014), http://www.bracewellgiuliani.com/news-publications/updates/sdny-judge-orders-microsoft-produce-emails-stored-abroad (expounding upon the parties' arguments and Magistrate Judge Francis's decision).

21. *See SDNY Judge Orders Microsoft to Produce Emails Stored Abroad*, *supra* note 20 (explaining that Microsoft cautioned against the "judicial approval of this type of seizure" because it "could be met with potential backlash from the international community" since "the records [that the] DOJ sought were personal, third-party emails where the international customer had a reasonable expectation of privacy and not Microsoft's business records").

22. *See Microsoft Case*, *supra* note 15, at 467; *supra* note 3 and accompanying text.

23. *See Microsoft Case*, *supra* note 15, at 467, 470.

24. *See infra* Part III.C–D. Comity "refers both to legal policies that energize the rules of conflict of laws and to considerations of high international politics concerned with maintaining amicable and workable relationships between nations." Harold G. Maier, *Interest Balancing and Extraterritorial Jurisdiction*, 31 AM. J. COMP. L. 579, 589 (1983); *see also* Hartford Fire Ins. v. California, 509 U.S. 764, 817 (1993) (Scalia, J., dissenting) (referring to "prescriptive comity" as the respect afforded to foreign sovereignties by limiting the reach of the laws of the United States).

25. *See infra* Part II.A–B.

26. *See infra* Part II.C.

27. *See infra* Part III.

legislative reform, as well as a two-prong test, which judges can use to determine if a warrant should have extraterritorial jurisdiction.[28]

II. THE STORED COMMUNICATIONS ACT, FOURTH AMENDMENT, AND OTHER POTENTIAL PROTECTIONS

While the insufficiencies of the SCA are not recent discoveries,[29] the decision in the *Microsoft Case*, discussing the jurisdictional reach of the SCA, demonstrated the statute's flaws on an international scale.[30] This Part introduces the history leading up to the enactment of the SCA and the statute itself.[31] This Part also discusses legal doctrines and procedures that work in conjunction with the SCA.[32]

A. The Stored Communications Act

The SCA is Title II of the Electronic Communications Privacy Act of 1986 ("ECPA").[33] The ECPA was enacted "to protect against the unauthorized interception of electronic communications"[34] and to provide additional privacy rights in electronic communications.[35] The SCA specifically applies to third-party electronic communication service providers and prohibits them from sharing any of their customers' stored electronic communications.[36] Thus, the statute prohibits companies like

28. *See infra* Part IV.

29. *See, e.g.*, Kerr, *supra* note 12, at 1233. For years, academics have highlighted some problems that arise under the SCA, ranging from its lack of privacy protection to its outdated terminology. For further discussion on these issues, see Patricia L. Bellia, *Surveillance Law Through Cyberlaw's Lens*, 72 GEO. WASH. L. REV. 1375, 1395 n.121 (2004), and Kerr, *supra* note 12, at 1233.

30. *See Microsoft Case*, *supra* note 15, at 466, 475-76; *infra* Part III.A.

31. *See infra* Part II.A.

32. *See infra* Part II.B–C.

33. The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 2510–2522 (1986); *see also Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. § 2510-22*, JUST. INFO. SHARING, https://it.ojp.gov/default.aspx?area=privacy&page=1285 (last updated July 30, 2013) (explaining that the SCA is one of three different titles in the ECPA).

34. S. REP. NO. 99-541, at 1 (1986).

35. *Id.* at 1-3. In this report, Congress acknowledged that stored communications needed additional safeguards that were not covered by the Fourth Amendment. *Id.* at 3; *see also* Bellia, *supra* note 29, at 1396-97, 1413 (explaining that Congress enacted the SCA to protect electronic information that was not previously protected by the Fourth Amendment).

36. 18 U.S.C. § 2702(a) (2012); *see also* 18 U.S.C. § 2702(a)(3) ("[A] provider of remote computing service or electronic communication service to the public shall not knowingly divulge a record or other information pertaining to a subscriber to or a customer of such service . . . to any governmental entity."). Emails stored on an ISP's server that have not been opened yet are considered to be in storage. Mark D. Young, *Electronic Surveillance in an Era of Modern Technology & Evolving Threats to National Security*, 22 STAN. L. & POL'Y REV. 11, 18 (2011).

Yahoo or Google from sharing a user's stored emails.[37] The SCA was enacted as a response to the public's ever-increasing use of electronic communications, which were not adequately protected by the Fourth Amendment.[38]

The Fourth Amendment traditionally protects individuals from warrantless searches and seizures; however, the sphere of protection afforded by the Fourth Amendment does not necessarily extend to documents stored in cyberspace.[39] Thus, the SCA was enacted to address the gaps in traditional Fourth Amendment interpretations by creating privacy protections for users of electronic communications.[40] Additionally, parts of the SCA were enacted to help law enforcement officers obtain electronically stored information during criminal investigations.[41] Under § 2703 of the SCA, law enforcement officers may request electronically stored information from the ISP that holds it.[42] This can be done with an administrative subpoena, a court order, or a warrant.[43] Depending on how the information is requested, the prerequisites necessary to obtain the information and records that must be disclosed in reply will vary.[44]

1. Administrative Subpoenas

An administrative subpoena can compel an ISP to reveal limited non-content information pursuant to the SCA.[45] Issuing a subpoena requires authorization by a federal or state grand jury, trial subpoena, or

37. *See* Kerr, *supra* note 8, at 383 (explaining that the SCA provides privacy protections to email users).

38. S. REP. NO. 99-541, at 1-3; Kerr, *supra* note 12, at 1212. The SCA is the government's attempt to fill the holes left in Fourth Amendment jurisprudence and to protect network account holders' privacy rights. *See id.*

39. Kerr, *supra* note 12, at 1209-10 (explaining that the Fourth Amendment protects individuals from an unreasonable search of physical spaces such as our homes, papers, and other tangible items, but not necessarily of our "virtual homes"); *see also* S. REP. NO. 99-541, at 1-3 (explaining the law's general need for clarity, reform, and added protections due to evolving technology).

40. *See* Kerr, *supra* note 12, at 1212-13.

41. 18 U.S.C. § 2703 (2012); *see also* Paul M. Schwartz, *Reviving Telecommunications Surveillance Law*, 75 U. CHI. L. REV. 287, 298-99 (2008) (noting that an SCA warrant can be issued for any criminal investigation, not just "a set of predicate offenses").

42. § 2703(a).

43. § 2703(b)(1)(A), (B)(i)–(ii).

44. § 2703(a)–(d); *see infra* Part II.A.1–3 (explaining, in detail, the requirements to obtain each instrument and the records that must be disclosed).

45. § 2703(b)(1)(B)(i), (c)(2). Generally speaking, agencies have the authority to issue subpoenas in furtherance of investigations and adjudicative matters. CHARLES DOYLE, CONG. RESEARCH SERV., RL 33321, ADMINISTRATIVE SUBPOENAS IN CRIMINAL INVESTIGATIONS: A BRIEF LEGAL ANALYSIS 6 (2006).

statute.[46] The SCA does not impose any additional requirements to obtain a subpoena beyond the usual standards that administrative agencies and law enforcement officers follow.[47] Further, the scope of the subpoena must only be reasonable to avoid Fourth Amendment challenges.[48] Agencies may send subpoena requests to any person or entity holding relevant information.[49]

Once a subpoena is issued for an account, the ISP is obligated to disclose the name, address, Internet Protocol connection records, and payment information used in connection with that account.[50] An administrative subpoena may also compel the production of any unopened emails that are more than 180 days old,[51] as well as any opened emails irrespective of how old they are.[52] Law enforcement officers do not need to give any prior notice to account holders when requesting these records from the ISP.[53] It is also possible for a subpoena to compel disclosure of the "contents" of electronically stored information.[54] This has been interpreted to mean that a subpoena can compel an ISP to disclose the information in both the subject line and the body of an email.[55] However, when a subpoena requests the contents of the email, law enforcement officers shall give the account holder prior notice.[56]

---

46. § 2703(b)(1)(B)(i).

47. *Microsoft Case*, *supra* note 15, at 469. Under the Administrative Procedure Act, an administrative agency and challenging parties are able to issue subpoenas to witnesses asking for their cooperation in pending suits. 5 U.S.C. § 555(d) (2012).

48. DOYLE, *supra* note 45, at 9. This standard usually requires the following elements to be satisfied: (1) the investigation has a legitimate purpose; (2) the subpoena does not violate the terms of the agency's authorizing statute; (3) the requested documents are relevant to the investigation; (4) the agency has not already obtained the information being sought; and (5) the subpoena will not be an abuse of the court's process. *See id.* at 10.

49. § 555(d). Where the proceeding is for enforcement, the court will order the witness to appear or produce the requested evidence. *Id.*

50. § 2703(c)(2); *Microsoft Case*, *supra* note 15, at 468.

51. § 2703(a); *Microsoft Case*, *supra* note 15, at 468.

52. § 2703(b)(1)(B)(i); *Microsoft Case*, *supra* note 15, at 468-69, 469 n.2.

53. § 2703(c)(3) ("A governmental entity receiving records or information under this subsection is not required to provide notice to a subscriber or customer.").

54. § 2703(a)–(b); *see also* Kerr, *supra* note 12, at 1228 (explaining that the SCA takes its definition of "contents" from the Wiretap Act). The Wiretap Act defines "contents" as the "substance" of the electronic communication. 18 U.S.C. § 2510(8) (2012).

55. *Microsoft Case*, *supra* note 15, at 467. In this case, Magistrate Judge Francis explained that emails include both non-content information and content information. *Id.* Information such as the sender's email address, the recipient's email address, and the time and date that the email was sent are considered non-content information. *Id.* Content information includes the words written in the subject line of an email, as well as the message typed in the body of the email. *Id.*

56. § 2703(b)(1)(B)(i); *Microsoft Case*, *supra* note 15, at 469.

2. Court Orders

A court order is another method of obtaining limited non-content information and provides more information than an administrative subpoena.[57] If a law enforcement officer obtains a court order, the officer is entitled to all of the information that is available under the subpoena, as well as "record[s] or other information pertaining to a subscriber . . . or customer."[58] This information includes historical logs that reveal the email addresses with which a user has communicated.[59] Further, a law enforcement officer has a greater burden to meet when seeking a court order than when seeking a subpoena[60]: the officer must show that there are "specific and articulable facts showing that there are reasonable grounds to believe that the contents . . . are relevant to an ongoing criminal investigation."[61]

3. Stored Communications Act Warrants

A search warrant pursuant to § 2703(a) of the SCA permits a law enforcement officer to all information subject to production under both administrative subpoena and court order, as well as the contents of any unopened emails that are stored for less than 180 days.[62] Further, law enforcement officers are not required to give the account holder prior notice that this information is being accessed.[63] A warrant pursuant to this section is often referred to as an "SCA warrant."[64] Since this method reveals the most information, obtaining an SCA warrant imposes a much greater burden on the government than in obtaining a subpoena or court order.[65] To obtain an SCA warrant, law enforcement officers must follow the same protocol as for traditional search warrants under rule 41 of the *Federal Rules of Criminal Procedure* ("Rule 41"), which requires officers to have probable cause.[66]

---

57. *Microsoft Case*, *supra* note 15, at 469.

58. § 2703(c)(1)(B); *Microsoft Case*, *supra* note 15, at 469.

59. *Microsoft Case*, *supra* note 15, at 469.

60. *In re* Application of the U.S. for an Order Directing a Provider of Elec. Commc'n Servs. to Disclose Records to the Gov't, 620 F.3d 304, 314 (3d Cir. 2010) [hereinafter *In re* Application of the U.S.]; DOYLE, *supra* note 45, at 9. The law enforcement officer need not establish probable cause, but the standard is higher than a subpoena. *In re* Application of the U.S., supra, at 314-15. This intermediate burden of proof was implemented to protect against overzealous law enforcement officers. *Id.*

61. § 2703(d); *see also In re* Application of the U.S., *supra* note 60, at 313 (denying that § 2703(d) requires proving probable cause and holding that a lower burden applies).

62. *Microsoft Case*, *supra* note 15, at 470.

63. § 2703(b)(1)(A).

64. *See, e.g.*, *Microsoft Case*, *supra* note 15, at 470.

65. *See In re* Application of the U.S., *supra* note 60, at 313.

66. § 2703(a); *Microsoft Case*, *supra* note 15, at 470; FED. R. CRIM. P. 41(d)(1) (mandating

B. Traditional Searches and Seizures in the United States

U.S. citizens have always relied upon the Fourth Amendment to protect them from unreasonable government searches and seizures.[67] Additionally, Rule 41 helps protect the public against unreasonable intrusions by defining the prerequisites to obtain a search warrant.[68] However, the Fourth Amendment needs to evolve in light of developments in modern technology.[69]

1. The Fourth Amendment in the Twenty-First Century

The Fourth Amendment[70] is a fundamental protection in the U.S. Constitution that prohibits the government from unlawfully searching or seizing information where there is a reasonable expectation of privacy.[71] The framers of the Fourth Amendment sought to protect individuals' privacy interests from unreasonable government intrusions.[72] Traditionally, this expectation of privacy has applied to physical places, like our homes.[73]

However, once an individual willingly shares information with a third party, the Fourth Amendment protections no longer apply.[74] This

---

that law enforcement officers demonstrate probable cause before a warrant will be issued); *see also In re* Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (concluding that Congress specifically intended that the procedures in Rule 41 for "obtaining and issuing search warrants" apply to § 2703(a)).

67. *See* Kerr, *supra* note 12, at 1209.

68. *See* FED. R. CRIM. P. 41; *infra* Part II.B.2.

69. *See infra* Part II.B.1.

70. U.S. CONST. amend. IV. The Fourth Amendment reads as follows:

> 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.

Id. The Fourth Amendment can be bifurcated into two separate clauses: one protecting from unreasonable searches and seizures by government agents and the other requiring probable cause for the issuance of a warrant. *Investigations and Police Practices*, 38 GEO. L.J. ANN. REV. CRIM. PROC. 3, 3 (2009).

71. U.S. CONST. amend. IV; Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); *see also* MARK G. MILONE, INFORMATION SECURITY LAW § 10.01 (2016) (explaining that there is no rigid rule to determine if someone has a reasonable expectation of privacy, but rather a two-part test that considers subjective and objective expectations).

72. *See* MILONE, *supra* note 71, § 10.01; *see also Investigations and Police Practices*, *supra* note 70, at 3 (explaining that the Fourth Amendment prohibits unreasonable searches and seizures).

73. Kerr, *supra* note 12, at 1209; *Investigations and Police Practices*, *supra* note 70, at 27 (explaining that a search warrant protects an individual against unjustified governmental intrusion of his home and possessions, thereby preserving the individual's privacy interest).

74. *Katz*, 389 U.S. at 351 ("What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); *see also* United States v. Miller, 425 U.S. 435, 438, 443 (1976) (holding that the government did not violate the defendant's Fourth

distinction has become unclear with advancements in electronic communications[75] because information is shared ipso facto with a third party (the ISP) once stored on a server.[76] Courts are just beginning to consider whether there is a reasonable expectation of privacy when communicating through an ISP.[77]

2. Federal Rule of Criminal Procedure 41

Rule 41 provides the procedural requirements necessary to obtain a search warrant.[78] First, a neutral and impartial judge must have the jurisdictional authority to issue a warrant in that district.[79] Second, a judge may only issue a warrant if the property to be searched and seized is evidence, or the fruits, of a crime.[80] Third, there must be a nexus between the property being seized and the criminal behavior under investigation.[81] Finally, a judge must determine whether probable cause exists.[82] Probable cause exists when there is a "reasonable ground for belief of guilt"[83] or "suspect[ing] that a person has committed or is committing a crime."[84] To determine if probable cause exists, a judge will consider the totality of the circumstances surrounding an

---

Amendment rights when it obtained financial documents from the defendant's bank because defendant had voluntarily conveyed that information to a third party).

75. *See In re* U.S. for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to Not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1213 (D. Or. 2009) (describing that when a person accesses the Internet, the information does not remain in the physical home, but rather remains on a server owned by ISPs, complicating the application of the Fourth Amendment).

76. *See* Kerr, *supra* note 12, at 1209-11 ("Our most private information ends up being sent to private third parties and held far away on remote network servers.").

77. *See, e.g.*, Guest v. Leis, 255 F.3d 325, 336 (6th Cir. 2001) (holding that computer users do not have a reasonable expectation of privacy because they are sharing such information with system operators); *see also* United States v. Maxwell, 45 M.J. 406, 418 (C.A.A.F. 1996) (stating that once an email is sent through a server, like America Online, the reasonable expectation of privacy may be destroyed because of third-party access). *But see* State v. Reid, 914 A.2d 310, 313, 317 (N.J. Super. Ct. App. Div. 2007) (holding that under the relevant state constitution, the defendant created a reasonable expectation of privacy in her identity by use of an anonymous ISP account number).

78. *See* FED. R. CRIM. P. 41(b)–(e).

79. FED. R. CRIM. P. 41(b); *Investigations and Police Practices*, *supra* note 70, at 21-22.

80. FED. R. CRIM. P. 41(c)(1)–(2); *Investigations and Police Practices*, *supra* note 70, at 22.

81. Warden, Md. Penitentiary v. Hayden, 387 U.S. 294, 307 (1967).

82. FED. R. CRIM. P. 41(d)(1); *Investigations and Police Practices*, *supra* note 70, at 13.

83. Brinegar v. United States, 338 U.S. 160, 175 (1949).

84. *Probable Cause*, BLACK'S LAW DICTIONARY (9th ed. 2009); *cf.* Ornelas v. United States, 517 U.S. 690, 695 (1996) ("Articulating precisely what . . . 'probable cause' mean[s] is not possible. [It is a] commonsense, nontechnical conception[] that deal[s] with 'the factual and practical considerations of everyday life on which reasonable and prudent men, not legal technicians, act.'" (quoting Illinois v. Gates, 462 U.S. 213, 231 (1983))).

incident.[85] There are no per se rules when deciding if probable cause exists.[86] Furthermore, it is a well-settled principle of law that establishing probable cause requires a lesser showing than that required to obtain a conviction.[87]

C. *Extraterritorial Jurisdiction*

With the invention and evolution of email, questions arise regarding the constitutional protections afforded to email account holders, especially when emails are stored on data servers overseas.[88] One possibility is for courts to conclude that the SCA has extraterritorial jurisdiction, meaning that the statute is applicable to conduct occurring outside of the United States.[89] Extraterritorial jurisdiction also allows the United States to exercise jurisdiction over parties who are not physically within the United States.[90] However, there is a presumption that Congress intends statutes to apply only to those within the United States.[91] The Supreme Court has said that Congress should only legislate extraterritorially if there is a reasonable basis for exercising jurisdiction over the person or activity located outside the United States, and it

85. *Gates*, 462 U.S. at 230-31.

86. *Investigations and Police Practices*, *supra* note 70, at 24.

87. *Brinegar*, 338 U.S. at 175 (citing Locke v. United States, 11 U.S. 339, 348 (1813)) (explaining that the phrase probable cause, according to its common understanding, means less evidence is required than is required for "condemnation").

88. *Id.*; *see supra* Part II.B.1; *infra* Part III.A.

89. *See* EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991); *see also* Swanson, *supra* note 14, at 721 (debating whether a court could exercise jurisdiction over a server farm set on the high seas). This is also known as legislative jurisdiction or the "jurisdiction to prescribe." Hartford Fire Ins. v. California, 509 U.S. 764, 813 (1993) (Scalia, J., dissenting).

90. United States v. Aluminum Co. of Am., 148 F.2d 416, 443 (2d Cir. 1945) ("[I]t is settled law . . . that any state may impose liabilities, even upon persons not within its allegiance, for conduct outside its borders that has consequences within its borders which the state reprehends . . . ."); *see also* RESTATEMENT (SECOND) OF FOREIGN RELATIONS LAW OF THE UNITED STATES § 30(1) (AM. LAW INST. 1965) ("A state has jurisdiction to prescribe a rule of law (a) attaching legal consequences to conduct of a national of the state wherever the conduct occurs or (b) as to the status of a national or as to an interest of a national, wherever the thing or other subject-matter to which the interest relates is located."). *But see* Swanson, *supra* note 14, at 721-22. In his article, Swanson posits that law enforcement officers might be able to access the overseas servers based on the idea that it connects to local computers within the territorial boundaries. *Id.*

91. Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010) ("Congress ordinarily legislates with respect to domestic, not foreign, matters."); *Arabian Am. Oil Co.*, 499 U.S. at 248 (holding that Congress must express its "affirmative intention" for the statute to have an extraterritorial effect); *see also* Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454-55 (2007) (reinforcing the idea that U.S. legislation "does not rule the world").

should shy away from exercising jurisdiction in a way that might interfere with another nation's sovereignty.[92]

For a law enacted by Congress to affect those located outside U.S. borders, a reviewing court must first determine that exercising extraterritorial jurisdiction is reasonable.[93] If the exercise of extraterritorial jurisdiction is unreasonable, the inquiry ends there and jurisdiction may not be exercised.[94] Alternatively, if more than one nation has a reasonable interest in exercising jurisdiction, the court must decide *which* nation should exercise such jurisdiction.[95] A court or state must determine which nation has a greater interest in regulating such persons or activity.[96] Finally, if Congress does have jurisdiction to regulate the matter, a court must then interpret the statute to decide the underlying issue.[97] To do so, a judge first looks at the plain meaning of the language in the law.[98] If the plain meaning of the language is clear and unambiguous, the court has a duty to enforce that meaning.[99] However, if the language in the statute is ambiguous,[100] a judge may

92. F. Hoffman-La Roche Ltd. v. Empagran S.A., 542 U.S. 155, 164-65 (2004) (stating that U.S. laws should "avoid unreasonable interference with the sovereign authority of other nations"); *see also Hartford Fire Ins.*, 509 U.S. at 818 (Scalia, J., dissenting) ("Under the Restatement, a nation having some 'basis' for jurisdiction to prescribe law should nonetheless refrain from exercising that jurisdiction 'with respect to a person or activity having connections with another state when the exercise of such jurisdiction is unreasonable.'"). In *Hartford Fire Insurance*, Justice Scalia presented two important canons of statutory interpretation: (1) unless Congress shows otherwise, its legislation is only meant to apply within the United States; and (2) a legislative act should not be interpreted in such a way that it will violate the laws of another country, if there is any other possible interpretation available. *Hartford Fire Ins.*, 509 U.S. at 814-15 (Scalia, J., dissenting).

93. RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 (AM. LAW INST. 1987). Whether jurisdiction is unreasonable will be determined by many factors, including the relation of the activity to the territory trying to assert jurisdiction, the nationality or relation of nationality between the state and the person responsible for the activity, the importance of regulation to the state, and the likelihood of creating conflict with another state when exercising jurisdiction. *Id.* Section 403(3) of the *Restatement (Third) of the Foreign Relations Law of the United States* explains that when it is not unreasonable for two states to exercise jurisdiction, but both exercising jurisdiction would cause conflict, each state has an obligation to measure its own interest in exercising jurisdiction against the other state's interest. *Id.* The state should defer to the other if the other state's interest is clearly greater. *Id.*

94. *See id.*

95. *Id.*

96. *Hartford Fire Ins.*, 509 U.S. at 821 (Scalia, J., dissenting); RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403. Applying such test is also referred to as a "conflict-of-laws analysis." *Hartford Fire Ins.*, 509 U.S. at 821 (Scalia, J., dissenting).

97. *See* EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991).

98. *See* Hartford Underwriters Ins. v. Union Planters Bank, 530 U.S. 1, 6 (2000) (stating that courts must enforce the plain meaning of the statute's language unless such interpretation would produce an "absurd" result).

99. *See* Hughes Aircraft Co. v. Jacobson, 525 U.S. 432, 438 (1999).

100. Statutory language "is ambiguous if it is 'capable of being understood in two or more

look toward legislative history or canons of interpretation to determine if Congress intended the statute to have extraterritorial jurisdiction.[101]

III. THE FLAWS OF THE STORED COMMUNICATIONS ACT

While the SCA was innovative when enacted, it has become clear that it no longer sufficiently safeguards Fourth Amendment privacy rights in the twenty-first century.[102] Technology has advanced while the statute, which still uses outdated technological terms from 1986, has not.[103] Further, many issues have arisen since the SCA's enactment, such as debates over its jurisdictional reach, questions about its interaction with existing law, and confusion over textual ambiguities.[104] The statute, in its current form, is wildly complex and needs legislative reform.[105] Professor Orin Kerr has pointed out as follows:

> The SCA is not a catch-all statute designed to protect the privacy of stored Internet communications; instead it is narrowly tailored to provide a set of Fourth Amendment-like protections for computer networks. Unfortunately, some judges have had a difficult time realizing this, and have twisted the statute to do things that it was never intended to do.[106]

Since the statute is difficult to construe, judges have had contradicting interpretations of the SCA, resulting in a lack of uniformity regarding the statute's applicability.[107] The *Microsoft Case*, which was recently decided in the Southern District of New York, discussed

---

possible senses or ways.'" *In re* U.S. for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to Not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1216 (D. Or. 2009) (quoting Chickasaw Nation v. United States, 534 U.S. 84, 90 (1992)).

101. *See Chickasaw Nation*, 534 U.S. at 94 (explaining that canons of statutory interpretation "are designed to help judges determine the Legislature's intent as embodied in particular statutory language"). *But see* Boureslan v. Arabian Am. Oil Co., 857 F.2d 1014, 1018-19 (5th Cir. 1988) (explaining that courts shall not substitute legislative history for the language of the statute).

102. *See* Kerr, *supra* note 12, at 1233-34.

103. Orin S. Kerr, *Lifting the "Fog" of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 821 (2003) (explaining how the SCA uses technology terms of the 1980s and that this increases the difficulty in interpreting it). The terminology is now largely outdated when applied to mass storage of data by ISPs. *See id.* at 821.

104. *See infra* Part III.A–D.

105. *See* Kerr, *supra* note 12, at 1233.

106. *Id.* at 1214.

107. *Compare Microsoft Case*, *supra* note 15, at 472, 474, *with* Zheng v. Yahoo! Inc., No. C-08-1068, 2009 WL 4430297, at *3, *4 (N.D. Cal. Dec. 2, 2009) (stating that the ECPA does not express any Congressional intent for extraterritorial application and, therefore, does not apply outside of the United States).

some of these issues and showed many of the deficiencies of the SCA in its current form.[108]

A. *The* Microsoft Case

Magistrate Judge James C. Francis, presiding in the Southern District of New York, recently issued a search warrant compelling Microsoft to release a customer's emails stored on a server in Dublin, Ireland.[109] Microsoft partially complied by releasing a limited amount of non-content information stored within the United States, but it refused to share information stored on its server in Ireland.[110] In objecting, Microsoft posited that a search occurs where the information is stored, not where it is viewed.[111] This theory was also consistent with Microsoft's contention that an SCA warrant is more like a traditional search warrant and should be executed in strict accordance with the Rule 41 warrant requirements.[112] Based on Microsoft's arguments, SCA warrants would not have their own extraterritorial jurisdictional basis and would thus need to be enforced with the help of an MLAT.[113]

In his analysis, Magistrate Judge Francis largely rejected Microsoft's position.[114] He began by interpreting the language of the statute,[115] where he found an ambiguity on its face.[116] He explained that the statute "is ambiguous in at least one critical respect."[117] The language in the statute that refers to Rule 41 could be read consistently with Microsoft's interpretation of the statute, which would mean the warrant lacks any extraterritorial effect.[118] However, the language could also be read to mean that Rule 41 provides the procedural mechanisms

108. *See infra* Part III.A.

109. *SDNY Judge Orders Microsoft to Produce Emails Stored Abroad*, *supra* note 20.

110. *Microsoft Case*, *supra* note 15, at 468.

111. *Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, CDT (July 30, 2014), https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad (comparing the government and Microsoft's contradicting views of where a search occurs).

112. *Microsoft Case*, *supra* note 15, at 470.

113. *Id.* at 470, 474; *Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111.

114. *Microsoft Case*, *supra* note 15, at 470, 474.

115. *Id.* at 470. This makes sense since courts should only turn to legislative intent and other methods of interpreting the meaning of a statute if the statute's language is ambiguous. *See* Boureslan v. Arabian Am. Oil Co., 857 F.2d 1014, 1018-19 (5th Cir. 1988).

116. *Microsoft Case*, *supra* note 15, at 470. Magistrate Judge Francis found the ambiguity to be encapsulated in the phrase "using the procedures described in the Federal Rules of Criminal Procedure." *Id.*

117. *Id.*

118. *Id.*

necessary for an SCA warrant, but the warrant takes its substantive rules from elsewhere.[119]

To clarify this ambiguity, Magistrate Judge Francis turned to the policy reasons behind the SCA's enactment.[120] After describing the lack of protection afforded by the Fourth Amendment, he quickly arrived at the conclusion that a warrant issued under § 2703(a) "is a hybrid: part search warrant and part subpoena."[121] The hybrid nature of an SCA warrant is due to the fact that law enforcement officers apply for it like they would a regular search warrant under Rule 41,[122] yet it "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 email[s]."[123]

Next, Magistrate Judge Francis addressed some of the "scant" legislative history surrounding the enactment of both the ECPA and the SCA.[124] For support, he relied on a Senate report on the ECPA discussing the massive amounts of data already stored by remote third-party operators in 1986.[125] He suggested that although Congress did not specifically discuss the idea of extraterritoriality, the awareness of remote third-party operators in 1986 "reflected an understanding that information was being maintained remotely by third-party entities."[126]

Magistrate Judge Francis then turned to the Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act (USA PATRIOT ACT) Act of

---

119. *Id.*; *see, e.g.*, *In re* U.S. for a Search Warrant for Contents of Elec. Mail and for an Order Directing a Provider of Elec. Commc'n Servs. to Not Disclose the Existence of the Search Warrant, 665 F. Supp. 2d 1210, 1219 (D. Or. 2009) (explaining that the ambiguity in the term "issued" could be interpreted as limiting the procedures available under § 2703(a) or could have been used as a "shorthand for the process of obtaining, issuing, executing, and returning a warrant, as described in Rule 41").

120. *Microsoft Case*, *supra* note 15, at 471.

121. *Id.* Magistrate Judge Francis's characterization of an SCA warrant as a hybrid is similar to Professor Kerr's description of a § 2703(d) court order:

> [A §] 2703(d) order . . . is something like a mix between a subpoena and a search warrant. To obtain the order, the government must provide specific and articulable facts showing that there are reasonable grounds to believe that the information to be compelled is relevant and material to an ongoing criminal investigation.

Kerr, *supra* note 12, at 1219.

122. *Microsoft Case*, *supra* note 15, at 471.

123. *Id.* What is peculiar about this interpretation is that nowhere in § 2703(a) does the statute refer to the warrant as a subpoena or a subpoena-like warrant. *See* 18 U.S.C. § 2703(a) (2012).

124. *Microsoft Case*, *supra* note 15, at 472.

125. *Id.* at 472-73 (quoting S. REP. NO. 99-541, at 3 (1986)).

126. *Id.* at 472. While this Senate report very well may reflect an understanding of remote third-party entities, there is no evidence to support the idea that the Senate meant to subject foreign third-party entities to this statute's jurisdiction. S. REP. NO. 99-541, at 1-3.

2001 ("Patriot Act")[127] to support the idea that information is located at an ISP's headquarters, "not the location of any server."[128] The Patriot Act allows for cross-jurisdictional warrants within the United States.[129] Therefore, Magistrate Judge Francis's interpretation makes the massive amounts of data stored around the world subject to the jurisdiction of an ISP's headquarters.[130] Under this reading, any email account that uses an ISP headquartered in the United States would be subject to an SCA warrant regardless of whether the account holder is personally subject to the warrant.[131]

Nevertheless, Magistrate Judge Francis misinterpreted the exact passage that he used to support this theory.[132] The Patriot Act simply allows for property located *within* the United States to be more easily accessible pursuant to a warrant.[133] Furthermore, the Patriot Act specifically states that the SCA *still* requires a search warrant.[134] It does not, in any way, amend the warrant requirement of the SCA.[135] Even if it did, the Patriot Act was enacted to protect against terrorism after the attacks of September 11, 2001.[136] Conversely, the investigation in the *Microsoft Case* involved narcotics trafficking, which does not necessarily have the same implications for national security.[137]

---

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

128. *Microsoft Case*, *supra* note 15, at 473-74. One reason to follow this line of thinking is that many of the large ISPs, like AOL and Yahoo, are located within the same jurisdictions, heavily burdening certain courts. *Id.* at 474 (citing Bellia, *supra* note 29, at 1454). This notion might be sensible when examined in a national context, but not necessarily in an international one. *See id.* at 474.

129. *Id.* at 473.

130. *See id.* at 474.

131. *See id.* at 473-74.

132. *See id.*; H.R. REP. NO. 107-236, pt. 1, at 57 (2001) ("18 U.S.C. § 2703(a) requires a search warrant to compel service providers to disclose unopened e-mails. This section *does not affect the requirement for a search warrant*, but rather attempts to address the investigative delays caused by the cross-jurisdictional nature of the Internet.").

133. *See* H.R. REP. NO. 107-236, at 57. The example used in the House of Representative's report demonstrates the ease with which law enforcement officers located in Boston seeking information located in California can obtain a "cross-jurisdictional warrant." *Id.* This Congressional report does not allude to an international search warrant. *See id.*

134. *See id.*

135. H.R. REP. NO. 107-236, at 57.

136. MICHEL E. BELEC ET AL., 703 THE EXTRA-JURISDICTIONAL REACH OF THE US PATRIOT ACT & ITS EFFECT ON CROSS-BORDER TRANSACTIONS 4 (ASS'N CORP. COUNSEL 2006).

137. *See* The Editorial Board, *Adapting Old Laws to New Technologies*, N.Y. TIMES (July 27, 2014), http://www.nytimes.com/2014/07/28/opinion/Must-Microsoft-Turn-Over-Emails-on-Irish-Servers.html.

Finally, Magistrate Judge Francis found that a search and seizure does not occur until a person actually views the information. Accordingly, in this case, there was no unconstitutional extraterritorial search since the information was viewed in the United States.[138] Magistrate Judge Francis's interpretation is flawed and could create a slippery slope concerning SCA warrants and data stored internationally.[139] His holding allows the government to circumvent the necessary and obligatory procedures set forth in an MLAT.[140] Avoiding the MLAT procedures offends international comity and sends a disrespectful message to foreign officials that U.S. law enforcement officers will execute the law as they see fit, regardless of any preexisting diplomatic agreements.[141] To justify his interpretation, Magistrate Judge Francis asserted that if the United States were to comply with the MLAT procedures, some information would be entirely outside the reach of U.S. law enforcement, and thus, the SCA must enjoy an extraterritorial application.[142] However, he failed to consider concepts like the "protective principle of jurisdiction."[143]

Most importantly, in his opinion, Magistrate Judge Francis interpreted the SCA in a manner that offends the Fourth Amendment.[144] Generally, a federal statute should not supersede the protections afforded

138. *Microsoft Case*, *supra* note 15, at 472.

139. *See Microsoft 'Must Release' Data Held On Dublin Server*, BBC (Apr. 29, 2014), http://www.bbc.com/news/technology-27191500 (discussing a European official's unhappiness with the holding of the Microsoft case because it allows for access "outside [the] formal channels of [international] co-operation").

140. *See id.*

141. *See id.*

142. *See Microsoft Case*, *supra* note 15, at 474-75. To bolster this statement, Magistrate Judge Francis mentioned that Google supposedly looked into developing server farms located in international waters, where no country has jurisdiction. *Id.* at 475.

143. *See* United States v. Juda, 797 F. Supp. 774, 777 (N.D. Cal. 1992). The protective principle is a constitutional basis to exert jurisdiction over a defendant located in international waters. *Id.* To exercise jurisdiction over a person or entity under this principle, there must be a "constitutionally sufficient nexus" between the defendant's conduct and the United States. *Id.*; *see also* Jennifer J. Berthiaume, United States v. Juda*: Fifth Amendment Due Process and Stateless Vessels On The High Seas*, 73 B.U. L. REV. 477, 480 (1993) (explaining that the protective principle "allows a nation to prosecute certain offenses committed outside its territory if these offenses threaten national security or otherwise interfere with governmental functions").

144. *See* Microsoft's Objections to the Magistrate's Order Denying Microsoft's Motion to Vacate in Part a Search Warrant Seeking Customer Information Located Outside the United States, *supra* note 4, at 3-4.

by the Constitution.[145] In fact, "[i]t would be manifestly contrary to the objectives" of the Constitution to interpret the Supremacy Clause as allowing Congress to enact laws without any regard for it.[146] Magistrate Judge Francis disregarded certain qualities in the SCA that suggest that an SCA warrant is meant to act like a typical search warrant.[147] The first indication that § 2703(a) should be interpreted as a traditional search warrant is that the statute uses the word "warrant" in conjunction with the procedures described in the *Federal Rules of Criminal Procedure*.[148] However, rather than erring on the side of caution, Magistrate Judge Francis implied, through his interpretation of the SCA, that the government may impinge on the constitutional protections afforded by the Fourth Amendment by allowing what appears to be a traditional search warrant to be executed extraterritorially.[149]

B. The Location of a Search or Seizure Under the Stored Communications Act

Some ISPs, like Microsoft, delete nearly all of the data from their servers in the United States once the information is securely stored in a foreign server.[150] Nevertheless, this information can easily be retrieved and viewed within the United States with minimal search efforts.[151] This brings up a second issue with the SCA—determining where a search and seizure actually occurs when the subject of the warrant is information stored in cyberspace.[152]

145. *See* U.S. CONST. art. VI, cl. 2 ("This constitution, and the laws of the United States which shall be made in pursuance thereof; and all treaties made, or which shall be made, under the authority of the United States, shall be the supreme law of the land . . . ."); *see also* Marbury v. Madison, 5 U.S. 137, 177 (1803) (holding a federal statute can never supersede the Constitution).

146. Reid v. Covert, 354 U.S. 1, 17 (1957).

147. *See* 18 U.S.C. § 2703(a) (2012).

148. *See id.*

149. *See Microsoft Case*, *supra* note 15, at 471-72, 474.

150. *Id.* at 467.

151. *Id.* at 468.

152. *See Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111. *But see In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (holding that there are actually two searches when dealing with computers—searching for the computer and searching the information stored on the computer).

One possible theory is that the search and seizure occurs where the data is physically stored.[153] If this is correct, then U.S. law enforcement officers would need to ensure that an SCA warrant is issued within the correct jurisdiction.[154] Under this theory, whether Congress intended for the SCA to have extraterritorial jurisdiction is critical.[155] Another theory is that the search and seizure occurs only where law enforcement officers view the information on the computer screen.[156] A final theory is that information is searched and seized not where it is stored or viewed but where the person who controls the information is located.[157] In fact, there is case law suggesting that the "test for production of documents is control, not location,"[158] but this precedent is based on subpoenas and not search warrants.[159]

C. *Extraterritorial Effects of the Stored Communication Act's Interpretation*

The language of the SCA does not address congressional intent on whether the statute has an extraterritorial reach.[160] The statute reads as follows:

> A governmental entity may require the disclosure by a provider of electronic communication service of the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less, only pursuant to a warrant issued using the procedures

153. *See Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111.

154. *See, e.g.*, *id.* This will only become an issue when a warrant is seeking to compel information that is stored outside the territorial jurisdiction of the United States, since the Patriot Act allows judges to issue warrants compelling information that is stored outside a judge's district but within the Untied States. *Let the Sun Set on PATRIOT—Section 220: "Nationwide Service of Search Warrants for Electronic Evidence,"* ELECTRONIC FRONTIER FOUND., https://w2.eff.org/patriot/sunset/220.php (last visited Apr. 10, 2016).

155. *See infra* Part III.C.

156. Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 551 (2005).

157. *Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111.

158. *Microsoft Case*, *supra* note 15, at 472 (quoting Marc Rich & Co. v. United States, 707 F.2d 663, 667 (2d Cir. 1983)).

159. *Marc Rich & Co.*, 707 F.2d at 667; Tiffany (NJ) LLC v. Qi Andrew, 276 F.R.D. 143, 147 (S.D.N.Y. 2011) ("[F]or the purposes of a Rule 45 subpoena, a document is within a witness's 'possession, custody, or control' if the witness has the practical ability to obtain the document."). If Magistrate Judge Francis's interpretation that the SCA warrant substantively acts like a subpoena is accepted, this control test will be the governing standard. *See Microsoft Case*, *supra* note 15, at 472.

160. *See* 18 U.S.C. § 2703(a) (2012).

> described in the Federal Rules of Criminal Procedure . . . by a court of competent jurisdiction.[161]

Scholars,[162] attorneys,[163] and judges[164] alike have debated whether Congress intended to create a warrant executed pursuant to Rule 41 or a warrant executed like a subpoena with this language.[165] Though the plain meaning and congressional intent are key in deciding whether a statute has extraterritorial jurisdiction,[166] there is little case law regarding the potential extraterritorial reach of an SCA warrant.[167] How the statute is interpreted greatly impacts just how much jurisdictional power the warrant gives law enforcement officials.[168]

1. A Stored Communications Act Warrant as Substantively Like a Traditional Search Warrant

It is well-established that judges do not have the statutory authority to issue warrants for foreign searches and seizures.[169] If Congress intended for an SCA warrant to be exercised as a traditional search

161. *Id.*

162. Recent Case, *Privacy Law—Stored Communications Act—District Court Holds that SCA Warrant Obligates U.S. Provider to Produce Emails Stored on Foreign Servers.*—In re Warrant to Search a Certain Email Account Controlled & Maintained by Microsoft Corp., 128 HARV. L. REV. 1019, 1023 (2015).

163. Reply Memorandum in Support of Microsoft's Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside the United States at 1-2, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained By Microsoft Corp., 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (No. 13-MJ-2814).

164. *Microsoft Case*, *supra* note 15, at 471. Professor Orin Kerr also notes the seeming inconsistency of the Eighth Circuit's actions in one case, where the court seemed to profess the standard of a warrant but apply the standard for a subpoena instead. Kerr, *supra* note 12, at 1211 n.18.

165. *Microsoft Case*, *supra* note 15, at 470-71.

166. *See supra* Part II.C.

167. *SDNY Judge Orders Microsoft to Produce Emails Stored Abroad*, *supra* note 20 (explaining that the *Microsoft Case* is the first case to decide on the application of a U.S. search warrant for data stored abroad); *see also* Zheng v. Yahoo! Inc., No. C-08-1068, 2009 WL 4430297, at *3 (N.D. Cal. Dec. 2, 2009) (stating that no other court had considered whether the ECPA applied extraterritorially prior to that point).

168. *See Microsoft Case*, *supra* note 15, at 468. Also, for the purposes of this section, when referring to a traditional search warrant, it is assumed that that the search occurs where the data is physically stored.

169. United States v. Bin Laden, 126 F. Supp. 2d 264, 275 & n.13 (S.D.N.Y. 2000) (explaining there are no statutory provisions that govern or provide for extraterritorial warrants); *see also* Reply Memorandum in Support of Microsoft's Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside the United States, *supra* note 163, at 1-2 (highlighting the fact that there are no U.S. cases interpreting an SCA warrant to be executed like a subpoena).

warrant, the warrant cannot have extraterritorial jurisdiction because Rule 41 does not include such language.[170] Using accepted methods of statutory interpretation, it seems clear that such information is accessible strictly through the use of a traditional search warrant.[171] Support for this theory is directly in the statute, which states that emails in storage for less than 180 days are accessible "*only* pursuant to a *warrant* issued using the procedures described" in Rule 41.[172]

Congress specifically used the term "warrant," rather than subpoena, in the statute and did not suggest any alternative interpretations of this word.[173] Nor is there any legislative history suggesting that Congress intended for a warrant to act like a subpoena.[174] Additionally, such information is accessible "only" pursuant to a warrant, indicating that there is no other method to obtain the information.[175] If Congress did not intend for an SCA warrant to reach into other sovereignties, there would be greater incentive for companies to begin storing larger amounts, or even all, of their data in less restrictive countries overseas, knowing that the information is outside the immediate reach of U.S. law enforcement officers.[176] The information would not be completely inaccessible, however, given that law enforcement officers may also rely on MLATs.[177]

---

170. *See* FED. R. CRIM. P. 41 (lacking language specifically granting extraterritorial jurisdiction).

171. *See supra* notes 98-101 and accompanying text.

172. 18 U.S.C. § 2703(a) (2012) (emphasis added).

173. *See* Reply Memorandum in Support of Microsoft's Motion to Vacate in Part an SCA Warrant Seeking Customer Information Located Outside the United States, *supra* note 163, at 1.

174. *See* H.R. REP. NO. 107-236, pt. 1, at 57 (2001). In its report, the House of Representatives committee specifically stated: "Title 18 U.S.C. § 2703(a) requires a *search warrant* to compel service providers to disclose unopened emails." *Id.* (emphasis added). The committee then explained that the Patriot Act was not intended to affect the search warrant requirement of the SCA; it was merely meant to decrease the time it previously took to obtain a warrant. *Id.*

175. *See* § 2703(a); *Only*, WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1577 (1993) (defining "only" as "just the one simple thing and nothing more or different"). Under the common understanding of the word "only," it appears as though a search warrant is the sole manner in which the information is accessible under the SCA. *See* § 2703(a); *Only*, *supra*.

176. *See* Shamoil T. Shipchandler, *Really Strange Bedfellows*, BRACEWELL (Aug. 5, 2014), http://www.bracewelllaw.com/blog/2014/08/05/really-strange-bedfellows.

177. *See Microsoft Case*, *supra* note 15, at 474; *see also infra* Part III.D (discussing procedures for executing a search warrant through the use of an MLAT and the complications that may arise).

2. A Stored Communications Act Warrant as Substantively Like a Subpoena

An alternative interpretation of the SCA is that an SCA warrant is meant to substantively act like a subpoena, with Rule 41 as simply the procedural vehicle to obtain the SCA warrant.[178] If this is the case, then when a person or entity is served with an SCA warrant, the test for compelling information under a subpoena would apply.[179] The requested documents would have to be produced regardless of their location, so long as they were under the control of the person or entity served with the SCA warrant.[180] This theory would increase the government's access to data stored overseas since many ISPs are headquartered in the United States and are therefore within its jurisdiction.[181]

When an SCA warrant is sent to an ISP, no law enforcement officers are physically present at the ISP's location to seize the information as there would be in a traditional search warrant scenario.[182] This supports the argument that an SCA warrant substantively behaves differently than a traditional search warrant by differentiating the characteristics between the two.[183] If Congress intended for the SCA warrant to be interpreted this way, then the government would not be

178. *Microsoft Case*, *supra* note 15, at 470; *see also In re* Search of Yahoo, Inc., No. 07-3194-MB, 2007 WL 1539971, at *5 (D. Ariz. May 21, 2007) (interpreting statutory amendments to mean Rule 41 should be applied to things that are procedural in nature). In *In re Search of Yahoo*, Judge Anderson first acknowledged that § 2703(a) used to read that a warrant under that section was valid pursuant to "a warrant 'under' the Rules of Criminal Procedure." *Id.* at *6. However, after the enactment of the Patriot Act, the language was changed so that a warrant is valid when issued "using the procedures described in" Rule 41. *Id.* at *5-6. Judge Anderson explained that the amendment created an ambiguity that lends itself to two reasonable conclusions: that all provisions of Rule 41 apply unconditionally or that Rule 41 only applies to the provisions of § 2703(a) that are procedural in nature. *Id.* at *5. By turning to the dictionary and common understandings of the word "procedure," Judge Anderson eventually concluded that Rule 41 only governs the procedural provisions of § 2703(a). *Id.*

179. *See Microsoft Case*, *supra* note 15, at 472.

180. *See id.* (quoting Marc Rich & Co. v. United States, 707 F.2d 663, 667 (2d Cir. 1983)); Government's Memorandum of Law in Opposition to Microsoft's Motion to Vacate Email Account Warrant at 10, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained By Microsoft Corp., 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (No. 13-MJ-2814) ("The compelled disclosure provisions set forth in § 2703 of the SCA do not alter the settled rule that a party located in the United States properly served with a compulsory demand for information as part of a federal criminal investigation is required to produce all responsive records within that party's possession, custody or control, regardless of where those records are located.").

181. *See Marc Rich & Co.*, 707 F.2d at 667. If the court has personal jurisdiction over the person or entity served, they will be able to "enforce obedience to . . . [a] subpoena." *Id.*

182. *See Microsoft Case*, *supra* note 15, at 471.

183. *See id.*

overstepping any jurisdictional boundaries or interfering with another nation's sovereignty because it would not be conducting an extraterritorial search and seizure. Rather, it would simply be compelling the production of information from a U.S. company pursuant to a subpoena.[184] Unfortunately, if this interpretation is accepted, the U.S. government would be infringing upon the comity owed to foreign nations[185] by essentially using the SCA warrant as a loophole to avoid well-established procedures and ratified MLATs.[186]

D. Mutual Legal Assistance Treaties and the Stored Communications Act

If an SCA warrant is not considered to substantively act like a subpoena, but rather like a warrant, then U.S. law enforcement officers have no choice but to turn to foreign nations for assistance in obtaining needed information.[187] An MLAT allows two countries to reciprocally "gather and exchange evidence and information to enforce public or criminal laws."[188] While MLATs can certainly be helpful in procuring information, they also force U.S. federal law enforcement to depend on foreign law enforcement to ensure compliance with U.S. statutes in foreign territories.[189] Generally, U.S. law enforcement officers "have no authority to conduct investigations, arrests, or seizures on their own beyond U.S. territorial limits."[190]

Furthermore, the foreign country typically has some discretion as to whether a U.S. search warrant should be honored.[191] If providing assistance would conflict with some essential public or national interest, then a party to an MLAT need not comply with a search warrant assistance request.[192] For example, in the *Microsoft Case* discussed earlier,[193] complying with the U.S. search warrant may have led to a

184. *See id.* at 472.

185. *See* Shipchandler, *supra* note 176.

186. *See id.*

187. *Microsoft Case*, *supra* note 15, at 474.

188. Amy E. Pope, *Lawlessness Breeds Lawlessness: A Case for Applying the Fourth Amendment to Extraterritorial Searches*, 65 FLA. L. REV. 1917, 1931 (2013).

189. *Id.*

190. *Id.*

191. *Microsoft Case*, *supra* note 15, at 474.

192. *Id.* at 474-75.

193. *See supra* Part III.A.

violation of the Irish Data Protection Acts and the EU Data Protection Directive.[194] This would give Ireland a reason to refuse to comply with the MLAT or help the United States execute a search warrant, since executing the warrant would violate one if its own laws.[195]

MLATs reinforce the principle of international comity.[196] If SCA warrants that indirectly allow for extraterritorial searches and seizures are enforced, then law enforcement could simply use a U.S. statute to avoid existing treaty obligations, which begs the question of why the United States enters into MLATs in the first place.[197] Since there is a presumption that a nation will not exercise its jurisdiction in a way that interferes with the sovereignty of another nation,[198] this interpretation flies in the face of existing treaties, international comity, and maintaining cordial relations with foreign nations.[199] In fact, European leaders have already admitted that they have concerns about the potential reach of SCA warrants following the decision in the *Microsoft Case*.[200]

IV. MODERNIZING THE STORED COMMUNICATIONS ACT TO REFLECT THE "SHRINKING" WORLD

The evolution of technology has prompted some to say that the world is shrinking.[201] While the conveniences and luxuries of electronic communication are enjoyed by many, the laws protecting the privacy of these relatively new methods of communication usually lag years, or even decades, behind how technology operates.[202] The SCA is in

194. Mary Minihan, *Microsoft Data Case May Have 'Very Serious' Implications—Minister Dana Murphy Says Ruling Could Create Legal Uncertainty for Consumers and Companies*, IRISH TIMES (Sept. 3, 2014), http://www.irishtimes.com/news/politics/microsoft-data-case-may-have-very-serious-implications-minister-1.1916834.

195. *See* JOSEPH BIDEN, MUTUAL LEGAL ASSISTANCE TREATIES WITH BELIZE, INDIA, IRELAND, AND LIECHTENSTEIN, S. EXEC. REP. NO. 107-15, at 3 (2002).

196. *See id.*; *see also* Hartford Fire Ins. v. California, 509 U.S. 764, 817 (1993) (Scalia, J., dissenting) (referring to "prescriptive comity" as the respect afforded to foreign sovereignties by limiting the reach of the laws of the United States).

197. *See* Shipchandler, *supra* note 176.

198. *See Hartford Fire Ins.*, 509 U.S. at 817 (Scalia, J., dissenting). A court will presume that a statute affords prescriptive comity to foreign nations because the court presumes that Congress exercises prescriptive comity when enacting laws. *Id.*; *see supra* Part II.C.

199. *See, e.g.*, Minihan, *supra* note 194.

200. *See, e.g.*, *Microsoft 'Must Release' Data Held On Dublin Server*, *supra* note 139.

201. *See* Rodger Dean Duncan, *Innovation: Expanding Horizons While Shrinking the World*, FORBES (Apr. 15, 2014, 1:41 PM), http://www.forbes.com/sites/rodgerdeanduncan/2014/04/15/innovation-expanding-horizons-while-shrinking-the-world. The ease with which we travel and communicate makes the world metaphorically feel like a smaller place. *Id.*

202. *See* Bellia, *supra* note 29, at 1385-88, 1396-97.

desperate need of reform, not only because of its outdated understanding of technology[203] but also because of its potential for unauthorized extraterritorial application.[204]

This Part suggests that the law should be reformed in a way that allows law enforcement agencies to obtain the information they seek, while safeguarding fundamental constitutional protections.[205] First, this Part explains whether the SCA warrant should be interpreted to be substantively more like a subpoena or a traditional search warrant.[206] It also addresses the dilemma of determining where the actual search and seizure occurs.[207] Second, this Part affirms the importance of MLATs and suggests reinforcing the use of MLATs when they exist by specifically mentioning them in the SCA.[208] Third, this Part explains how incorporating a jurisdictional balancing test when determining whether to execute an SCA warrant in a foreign country will help honor international comity on a macro level.[209] Finally, this Part applies the "minimum contacts" test on a micro level to the person or entity whose information is being sought by the government, as to ensure that the government is not overstepping their jurisdictional boundaries.[210]

A. Stored Communications Act Warrants Should Be Classified as Search Warrants and the Search Should Be Deemed to Occur Where the Data Is Located

Before any analysis or solution can be posited, it must first be established that an SCA warrant should not be classified as a subpoena or any form of "hybrid."[211] If Congress intended for the SCA warrant to substantively act as a subpoena, then it should amend the language of the statute to reflect that purpose.[212] Instead, it seems more likely, based on the plain language of the statute, that Congress intended for the SCA warrant to be executed as a traditional Rule 41 search warrant.[213]

---

203. Reforming the technological terminology in the statute is beyond the scope of this Note.

204. *See* Bellia, *supra* note 29, at 1396-97; *supra* Part III.C.

205. *See infra* Part IV.A–D.

206. *See infra* Part IV.A.

207. *See infra* Part IV.A.

208. *See infra* Part IV.B.

209. *See infra* Part IV.C.

210. *See infra* Part IV.D.

211. *Contra Microsoft Case*, *supra* note 15, at 471 (ruling that the SCA warrant is a hybrid between a subpoena and a warrant).

212. *See* Hartford Underwriters Ins. v. Union Planters Bank, 530 U.S. 1, 6 (2000) (stating that courts must enforce the plain meaning of a statute's language).

213. *See* 18 U.S.C. § 2703(a) (2012).

The next issue to address is where the search and seizure of data actually occurs.[214] This will turn on where the law considers the information to be physically located.[215] The information could be considered to be located where it is viewed on a computer screen,[216] where the server is located,[217] at the home or place of business of the email account user,[218] or at the ISP's headquarters where the ISP ultimately controls the data.[219] As a warrant, the standard for a subpoena—which looks to control and requires the recipient to produce the information regardless of the location—should not apply to an SCA warrant.[220] Rather, the most logical and strongest argument is that the search should occur where the data is stored and, therefore, where the server is located.[221]

B. Mutual Legal Assistance Treaties, When Available, Should Be the Authoritative Source in Determining Procedures for Executing Searches and Seizures in Foreign Countries

In the *Microsoft Case*, Magistrate Judge Francis's opinion described how burdensome the MLAT process is.[222] While this may be true, it should not give U.S. law enforcement officers the ability to ignore these obligations.[223] Magistrate Judge Francis opined that the United States had entered into MLATs with only sixty countries and concluded that, since U.S. law enforcement agencies do not have any other legislative methods to rely on when executing a search or seizure in other countries, Congress must have meant for the SCA to apply extraterritorially.[224]

---

214. *See* Kerr, *supra* note 8, at 416; *see also In re* Warrant to Search a Target Computer at Premises Unknown, 958 F. Supp. 2d 753, 757 (S.D. Tex. 2013) (ruling that two searches occur when executing the search and seizure of a computer: (1) searching for the computer and (2) searching the information stored on the computer).

215. *See Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111.

216. Kerr, *supra* note 156, at 551.

217. *Id.*

218. *See* Kerr, *supra* note 8, at 416. This location could be determined by obtaining the Internet Protocol or IP address of the email account holder. *Id.*

219. *See Microsoft Case*, *supra* note 15, at 472.

220. *See id.*

221. *See Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?*, *supra* note 111.

222. *See Microsoft Case*, *supra* note 15, at 474.

223. *See* Shipchandler, *supra* note 176; Drew Mitnick, *The Urgent Need for MLAT Reform*, ACCESSNOW (Sept. 12, 2014, 5:42 PM), https://www.accessnow.org/blog/2014/09/12/the-urgent-needs-for-mlat-reform.

224. *See Microsoft Case*, *supra* note 15, at 475.

However, when a judge considers whether to issue a § 2703(a) warrant, she should first determine whether an MLAT exists between the United States and the country in which law enforcement seeks to execute the search and seizure.[225] If there is an existing MLAT, U.S. law enforcement agencies must be bound by whatever procedures are outlined in the existing agreement.[226] Therefore, the language in the SCA should be changed to reinforce this notion.[227] Further, if the statute includes language that holds U.S. officers accountable to MLATs, it will provide further assurance toward international comity.[228] If the procedures are truly cumbersome, as some suggest,[229] then perhaps there should be a reform in the MLAT structure, rather than using the SCA or some other federal statute to skirt the issue.[230]

C. *Justice Scalia's Interpretation of the Conflict-of-Law Test Should Be Applied in Conjunction with the Stored Communications Act*

Although further procedures should be available to allow law enforcement agencies to obtain the information sought, it is still necessary to respect the sovereignty of foreign nations and the constitutional protections of U.S. citizens.[231] Although Justice Scalia's dissenting opinion in *Hartford Fire Insurance v. California* is not controlling, his interpretation of the conflict-of-law test in the *Restatement (Third) of Foreign Relations Law of the United States*

225. *But see id.*

226. *See* Haver v. Yaker, 76 U.S. 32, 35 (1869) (holding that the United States is bound by the terms of a treaty once the Senate ratifies it); *see also* Factor v. Laubenheimer, 290 U.S. 276, 293 (1933) (stating that treaties should be construed to secure equality and reciprocity between the contracting countries).

227. *See* 18 U.S.C. § 2703 (2012). It should be noted that such language is not imperative, as a treaty has full effect and force once ratified by the Senate. *See* U.S. CONST. art. II, § 2, cl. 2; *id.* art. VI, cl. 2 ("This constitution, and the laws of the United States which shall be made in pursuance thereof; and all *treaties* made, or which shall be made, under the authority of the United States, shall be the supreme law of the land." (emphasis added)). Including this language in the SCA will simply further memorialize the MLAT and ensure adherence to it.

228. *See* United States v. Davis, 767 F.2d 1025, 1033 (2d Cir. 1985) (recognizing that the United States must honor the sovereign respect owed to foreign nations and, as such, should not compel the production of information that would violate a foreign nation's laws).

229. *See* Pope, *supra* note 188, at 1931; *MLAT: A Four-Letter Word In Need Of Reform*, *supra* note 17.

230. However, discussing and analyzing MLAT reform is beyond the scope of this Note.

231. *See supra* Part II.B–C. It should be noted that the application of this standard should not begin until after it has already been determined that an MLAT between the United States and the foreign nation does not exist. *See supra* Part IV.B. Further, this standard should only be applied when law enforcement agencies are seeking data stored through an ISP organized pursuant to the laws of the United States, but the data server is located abroad.

("*Restatement (Third)*") is neutral and comprehensive.[232] Applying this test to the SCA should be the first step to ensure prescriptive comity and fairness when attempting to execute an SCA warrant in a foreign nation.[233] After determining that there is no MLAT between the United States and the foreign nation where the desired information is located, a judge should use the balancing test set forth in the *Restatement (Third)* and *Hartford Fire Insurance*.[234] This standard would ensure protection for constitutional rights and comity, forcing a judge to balance the legitimate interests of all involved in the case.[235]

When considering an application for an SCA warrant to be executed abroad, a judge should first consider if the United States has a reasonable interest in exercising extraterritorial jurisdiction.[236] Determining whether the United States has a reasonable interest in exercising jurisdiction will rely on the following non-exhaustive factors: the conduct's relation to the United States;[237] the extent of the effect of the conduct being regulated on the United States;[238] the nationality of the person responsible for the conduct;[239] the importance of issuing the warrant;[240] the expectations which might be impacted if the warrant is not issued;[241] "the importance of regulation to the international political, legal, or economic system";[242] whether exercising such jurisdiction would be consistent with the accepted norms of international law;[243] whether exercising jurisdiction would offend the sovereignty of another country;[244] and "the likelihood of conflict" with the foreign nation

232. *See* Hartford Fire Ins. v. California, 509 U.S. 764, 813-17 (1993) (Scalia, J., dissenting).

233. *See id.* at 817. This Note does not consider the outcome when foreign nations deny assistance in executing a U.S. search warrant abroad.

234. *See id.* at 818-19; RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403 (AM. LAW INST. 1987).

235. *See* Yahoo! Inc. v. La Ligue Contre Le Racisme Et, L'Antisemitisme, 145 F. Supp. 2d 1168, 1176-78 (N.D. Cal. 2001).

236. *See Hartford Fire Ins.*, 509 U.S. at 818 (Scalia, J., dissenting).

237. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2)(a).

238. *See id.*

239. *See id.* § 403(2)(b).

240. *See id.* § 403(2)(c). Section 403(2)(c) considers "the character of the activity to be regulated" and "the importance of [the] regulation." *Id.* Rather than the character of the activity being regulated, the court should mostly consider how important issuing the warrant is to the ongoing investigation, since the SCA refers to "ongoing criminal investigation[s]." *See* 18 U.S.C. § 2703(d) (2012).

241. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2)(d).

242. *See id.* § 402(2)(e).

243. *See id.* § 403(2)(f).

244. *See id.* § 403(2)(g).

storing the electronic information.[245] The answer to whether the United States has a reasonable interest will likely be affirmative since SCA warrants are only issued when a law enforcement officer can show probable cause.[246] In the unlikely event that the United States does not have a reasonable interest in exercising extraterritorial jurisdiction, the inquiry must end there—jurisdiction should not be exercised and a judge should not issue a warrant.[247]

However, if there is a reasonable interest, the inquiry must continue. A judge must next consider the interests of the foreign nation where the information is stored using the same factors listed above.[248] If, after weighing all of these factors, a judge concludes that the foreign nation has the greater interest, the United States should have to defer to that country's sovereignty and a judge should not issue a warrant.[249] Conversely, if a judge determines that the United States has the greater interest, she should then turn to the second prong of this Note's proposed test and consider the individual rights being affected.[250]

D. The Minimum Contacts Test for Personal Jurisdiction Should Be Applied in Conjunction with the Stored Communications Act

The second prong of the test suggested by this Note is to consider whether an individual email account holder has sufficient minimum contacts with the United States so that issuance of a warrant will not offend notions of due process.[251] This portion of the test is governed by the guiding principles set forth in *International Shoe Co. v. Washington*[252] and *Hanson v. Denckla*.[253] In determining whether such contacts exist, a judge should consider whether the person or entity holding an email account could have reasonably anticipated being "haled

245. *See id.* § 403(2)(h).

246. *See* 18 U.S.C. § 2703(a); FED. R. CRIM. P. 41(d)(1).

247. *See* Hartford Fire Ins. v. California, 509 U.S. 764, 819 (1993) (Scalia, J., dissenting).

248. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(2); *supra* notes 237-45 and accompanying text.

249. *See* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 403(3).

250. *See id.*; *infra* Part IV.D.

251. *See* United States v. Juda, 797 F. Supp. 774, 779 (N.D. Cal. 1992).

252. 326 U.S. 310, 316 (1945) (requiring that, for someone not physically present within the jurisdiction, there be "certain minimum contacts," so that being brought to court there does not "offend traditional notions of fair play and substantial justice").

253. 357 U.S. 235, 253 (1958) (holding that unilateral activity is not enough—the defendant must have "purposefully avail[ed himself] of the privilege of conducting activities within the forum state, thus invoking the benefits and protections of its laws").

into court,"[254] or in this case, subjected to a warrant.[255] If the person or entity's contact with the United States results from the unilateral acts of a third party, then extraterritorial jurisdiction should not be exercised.[256] This is because it would be unfair to force a person or entity to be under the jurisdiction of the United States if they are subject to the warrant solely due to someone else's conduct.[257]

Therefore, this Note suggests that courts should consider an email account holder's minimum contacts with the United States.[258] If the account holder maintains the requisite minimum contacts with the United States, then it would be reasonable for a court to issue a warrant.[259] This prong of the proposed test would help ensure fairness on a micro level by looking to the individual's conduct.[260]

V. CONCLUSION

When created, the SCA was a great effort to extend Fourth Amendment protections to newly emerging modes of communication.[261] However, Congress could not have foreseen the web of complexity and lack of protection that advancements in technology have created.[262] Case law and the resulting controversies surrounding warrants issued pursuant to § 2703(a) of the SCA have brought to light the areas that Congress failed to consider when drafting the SCA, such as whether the SCA was intended to have extraterritorial jurisdiction.[263] Courts have little guidance on this topic, and legislative reform is necessary to help answer this and other questions posed by the SCA.[264]

Thus, when a judge considers a warrant application for information stored on a data server overseas and the ISP is located in the United States, the two-prong test proposed in this Note should be applied.[265] This test considers the notions of international comity on a macro scale,

254. *See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

255. *See* 18 U.S.C. § 2703(b)(1)(A) (2012).

256. *See Hanson*, 357 U.S. at 253.

257. *See id.*

258. *See* United States v. Juda, 797 F. Supp. 774, 779 (N.D. Cal. 1992).

259. *See id.* Account holders may not have such minimum contacts, for example, when law enforcement officers are trying to obtain the emails or electronic data of people not directly involved in the suspected crime. *See Hanson*, 357 U.S. at 253.

260. *See* World-Wide Volkswagen Corp. v. Woodson, 444 U.S. 286, 297 (1980).

261. *See* S. REP. NO. 99-541, at 1-3 (1986).

262. *See* Kerr, *supra* note 12, at 1209, 1234.

263. *See supra* Part III.A, C.

264. *See supra* Part III.A–C.

265. *See supra* Part IV.

as well as an individual's rights on a micro scale.[266] Applying such a standard would help ensure diplomatic relations, which are more important than ever in this "shrinking" world, while also protecting the substantive individual protections that our Constitution holds dear.[267]

*Lindsay La Marca**

266. *See supra* Part IV.C–D.

267. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring); Maier, *supra* note 24, at 589; Duncan, *supra* note 201; *supra* Part IV.D.

* J.D. Candidate, 2016, Maurice A. Deane School of Law at Hofstra University; B.A. 2012, Stony Brook University. I would like to thank my parents, Frank and Kerry La Marca, my sister, Chelsea La Marca, and all of my friends for their unconditional love and support. I am grateful for this opportunity and the hard work of the Volume 44 Managing Board, Peter Guinnane, Leron Solomon, and Michael Senders, as well as the Volume 45 Managing Board, Joseph De Santis, Michelle Malone, and Susan Loeb, without whom the publication of this Note would not have been possible. I am also thankful for the words of wisdom that my faculty advisor, Professor James E. Hickey, and my Notes Editor, Ada Kozciz, provided to me throughout this process. Additionally, thank you to Thomas Haley, Nneka Nzekwu, Kathryn Barrett, and all *Hofstra Law Review* Staff Members who assisted in this publication. Last, but not least, I would like to thank Patrick Hatch for supporting me with endless patience throughout my journey in law school and continuing to motivate and inspire me to be the best version of myself, regardless of the endeavor.