Catholic University Journal of Law and Technology

Volume 26 | Issue 2 Article 8

2018

International Comity and the Non-State Actor, Microsoft: Why Law Enforcement Access to Data Stored Abroad Act (LEADS Act) Promotes International Comity

Sabah Siddiqui
Catholic University of America (Student)

Follow this and additional works at: https://scholarship.law.edu/jlt

 Part of the Comparative and Foreign Law Commons, Conflict of Laws Commons, Fourth Amendment Commons, International Law Commons, Internet Law Commons, and the Privacy Law Commons

Recommended Citation

Sabah Siddiqui, *International Comity and the Non-State Actor, Microsoft: Why Law Enforcement Access to Data Stored Abroad Act (LEADS Act) Promotes International Comity*, 26 Cath. U. J. L. & Tech 171 (2018).
Available at: https://scholarship.law.edu/jlt/vol26/iss2/8

This Comments is brought to you for free and open access by CUA Law Scholarship Repository. It has been accepted for inclusion in Catholic University Journal of Law and Technology by an authorized editor of CUA Law Scholarship Repository. For more information, please contact edinger@law.edu.

INTERNATIONAL COMITY AND THE NON-STATE ACTOR, MICROSOFT: WHY LAW ENFORCEMENT ACCESS TO DATA STORED ABROAD ACT (LEADS ACT) PROMOTES INTERNATIONAL COMITY

Sabah Siddiqui[+‡]

Over a third of the population in the United States has sent or read an email in the last twenty-four hours.[1] The email may have been well wishes from your

[+] J.D. Candidate, May 2019, The Catholic University of America, Columbus School of Law; B.A. 2011, The George Washington University. The Author is grateful to Professor Robert A. Destro for his guidance and support in the research and writing of this comment. The Author would like to thank her loving and supportive parents, Mohammed and Shahina K. Siddiqui, her brother, Dr. Jalal K. Siddiqui, and husband, Mihail D. Petrov. Additionally, the Author would like to thank the hard work and dedication of the associates and editors of the *Journal of Law and Technology* in preparation of this comment.

[‡] On April 17, 2018, the Supreme Court of the United States held that the case that is the subject of this paper, Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016) [hereinafter Microsoft II], will be dismissed due to mootness caused by the passage of the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act").The Law Enforcement Access to Data Stored Abroad Act ("LEADS Act"), discussed infra, and the CLOUD Act are quite different in nature. The LEADS Act, if it were passed, would have simply provided clarification that warrants under the Stored Communications Act ("SCA") would only apply to U.S. Citizens and not EU citizens. The LEADS Act would address the current conflicts issue more effectively than the CLOUD Act. The Author argues that the passage of the LEADS Act should be renewed in the interest of international comity. However, the CLOUD Act, enacted and signed into law on March 23, 2018, enables law enforcement to bypass the process proscribed in Mutual Legal Assistance Treaties ("MLATs") which would hinder international comity even more. This article argues for the U.S. to go through the MLATs process and if anything, countries should consider re-negotiating the MLATs to make them more amenable to each country's law enforcement needs. Because this paper is purely a conflicts of law analysis discussing the proper, extraterritorial application of the SCA, the Author solely focuses on the LEADS Act and does not discuss the CLOUD Act.

1 Frank Newport, *The New Era of Communication Among Americans*, GALLUP (Nov.

childhood friend, a confirmation of your wife's birthday present, an email from your boss asking for the status of a memorandum, or pertinent details related to a drug trafficking scheme. In the latter instance, a judge may issue United States law enforcement a probable cause warrant[2] under 18 U.S.C. 2703 for the content of these emails and a federal or state agent would serve this warrant on an email provider located in the United States.[3] However, the email service provider may have made the business decision— independent of the criminal or civil action investigation—to store the emails outside the United States.[4] Currently, as a result, email providers are refusing to turn over emails stored abroad, even if the U.S. governmental entity deems the emails necessary to the investigation.[5]

Except in national security-related criminal charges and investigations and in cases involving child pornography, email service providers can refuse to comply with a warrant requesting emails stored in their data centers located outside the

---

10, 2014), http://news.gallup.com/poll/179288/new-era-communication-americans.aspx.

2 Erica L. Danielsen, *Cell Phone Searches After Riley: Establishing Probable Cause and Applying Search Warrant Exceptions*, 36 PACE L. REV. 970, 976–77 (2016) (demonstrating that Magistrate judges may only issue search warrants based on probable cause). Some courts apply either the stringent two-prong *Aguilar-Spinelli* test, which provides that probable cause exists if the application for the warrant describes the "underlying circumstances necessary to enable the magistrate independently to judge of the validity of the informant's conclusion" and there must be enough information for the judge to determine the validity and reliability of the informant. *Id.* at 977. On the other hand, some courts apply a less stringent test than the *Aguilar-Spinelli*, which applies a "totality-of-the-circumstances" approach. *Id.*

3 Microsoft v. United States, 829 F.3d 197, 207 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (U.S. Oct. 16, 2017) (No. 17-2) [hereinafter Microsoft IV]; *see* 18 U.S.C. § 2703 (2016); Peter J. Henning, *Microsoft Case Shows the Limits of Data Privacy Law*, N.Y. TIMES (July 18, 2016), https://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html ("With a few keystrokes, electronic files can be whisked across the globe . . . While the files were in Ireland, that was more a product of how the company chose to store them rather than a conscious decision by the account owner to try to keep them outside the United States.").

4 Mark Scott, *Ireland Lends Support to Microsoft in Email Privacy Case*, N.Y. TIMES (Dec. 24, 2015), https://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/ (recognizing that, "[l]ike other American companies, Microsoft uses data centers around the world for cloud computing services like email and data storage.").

5 *See* Case Comment, *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., 15 F. Supp. 3d 466 (S.D.N.Y. 2014)*, 128 HARV. L. REV. 1019, 1025 n.51 (2015) (describing Microsoft's refusal to comply with a search warrant served by the U.S. government); Press Release, Dep't of Justice, Assistant Attorney General Leslie R. Caldwell Delivers Remarks Highlighting Cybercrime Enforcement at Center for Strategic and International Studies (Dec. 7, 2016), https://www.justice.gov/opa/speech/assistant-attorney-general-leslie-r-caldwell-delivers-remarks-highlighting-cybercrime.

United States.[6] This may have a detrimental effect on governmental investigations, especially if the service provider can easily access the information from the United States but it can also assist in maintaining international comity.[7] The issue presented in the upcoming Supreme Court case, *Microsoft II*, 829 F.3d 197 (2d Cir. 2016), is whether an Internet Service Provider (ISP) must comply with a warrant under the Stored Communications Act when the information under the ISPs' control is outside the United States.[8] Based on case law regarding extraterritorial application of federal statutes, the Supreme Court should rule in favor of the Government and reverse the appellate court decision.[9] In addition, Congress should amend the Secured Communications Act (SCA) to address the conflicts of law issues that arose because of advances in technology since SCA's enactment.[10]

Part I of this Article discusses the statutory background information regarding the issues presented in *Microsoft v. United States*.[11] Part II reviews the common law and procedural information related to the *Microsoft* cases and the potential

---

6 *See* Microsoft v. United States, 829 F.3d 197, 200 (2d Cir. 2016) [hereinafter Microsoft II] (explaining that Microsoft provided the customer's non-content information to the government but refrained from providing content information that was stored in Ireland); Brian G. Slocum, *Virtual Child Pornography: Does It Mean the End of the Child Pornography Exception to the First Amendment*, 14 ALB. L.J. SCI. & TECH. 637, 639 (2004) (highlighting the compelling governmental interest in protecting children by prohibiting child pornography); *see also* Lindsay La Marca, *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, 972 (2016) (stating that in addition to a company refusing to comply with a warrant, a country may not be obligated to provide the requested information if the information is held outside the U.S. and there is no Mutual Legal Assistance Treaty).

7 La Marca, *supra* note 6, at 971–72 (illustrating that Internet Service Providers ("ISPs") are beginning to store electronic information in "server farms" or "data centers" outside the U.S.); *see* Henning, *supra* note 3.

8 *See* 18 U.S.C. § 2701(a) (2016) (stating that a violation of the Stored Communications Act occurs when an entity has access to information stored with an electronic communication service and prevents authorized access to this electronic communication); Microsoft IV, 829 F.3d 197 (2d Cir. 2016), *cert. granted*, 138 S. Ct. 356 (U.S. Oct. 16, 2017) (No. 17-2).

9 *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U. L. REV. 267, 269–70 (2013) (stating the rationale for the varying court interpretations of the SCA is due to the differences in technology throughout the years); Randall S. Abate, *Dawn of a New Era in the Extraterritorial Application of U.S. Environmental Statutes: A Proposal for an Integrated Judicial Standard Based on the Continuum of Context*, 31 COLUM. J. ENVTL. L. 87, 88 (2006) (highlighting that there is a presumption against extraterritoriality that guides courts that are engaging in statutory interpretation).

10 *See* Medina, *supra* note 9, at 289 ("[A]ttempting to fit modern technology into the limited technological framework of 1986 has proven to be a daunting task.").

11 *See infra* Part I.

circuit split that may occur.[12] Next, Part III argues the Supreme Court should narrowly hold that a company providing email services in the United States must comply with a warrant issued under 18 U.S.C. 2703 when the user is a United States citizen, even if such data is stored outside the United States.[13] Finally, this Article argues in Part IV that the Supreme Court's decision would not resolve the issues presented, and there is a need for Congress to amend the SCA given the advancements in technology since its enactment and possible resolutions.[14]

I. STATUTORY BACKGROUND INFORMATION

A. Fourth Amendment

The Fourth Amendment protects the, "right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[15] It limits law enforcement from encroaching on constitutionally protected areas, including documents, by requiring a valid warrant to be issued based on probable cause with very few exceptions.[16] Correspondence via emails

---

12 *See infra* Part II.
13 *See infra* Part III.
14 *See infra* Part IV.
15 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.

U.S. CONST. amend. IV.

16 Ilana R. Kattan, *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, 624 (2011); *see* Dana T. Benedetti, *How Far Can the Government's Hand Reach Inside Your Personal Inbox?: Problems with the SCA*, 30 J. MARSHALL J. INFO. TECH. & PRIVACY L. 75, 76–77 (2013) (discussing the test for determining what is a constitutionally protected area and comparing emails to other forms of communication and highlighting that "this test has helped courts conclude that certain mediums of traditional communication, including telephone conversations and postal letters, are constitutionally protected by a reasonable expectation of privacy."); *see also* Johnson v. United States, 333 U.S. 10, 13 (1948) (holding that a valid warrant must be issued by a neutral and detached magistrate judge and that even the slightest deviation from the search warrant violates the Fourth Amendment); Katz v. United States, 389 U.S. 347, 357 (1967) ("[S]earches conducted outside the judicial process, without prior approval by judge or magistrate, are *per se* unreasonable under the Fourth Amendment—subject only to a few specifically established and well-delineated exceptions."); Microsoft II, 829 F.3d 197, 212 (2d Cir. 2016) ("Warrants issued in accordance with the Fourth Amendment thus identify discrete

can be viewed as analogous to physical documents.[17] However, when an individual sends an email from his or her home computer, neither the email nor its data is fully protected in the same manner as homes are under the Fourth Amendment.[18] If law enforcement seeks to enter an individual's home to search for a document that law enforcement reasonably suspects to be in a certain location in the home, then he or she must have a search warrant specifying the document and the location where they may reasonably find it.[19] However, the data embedded in emails does not receive the same protection.[20] Courts render non-content information, such as account information and IP addresses associated with emails stored by ISPs, outside the scope of protection under the Fourth Amendment because courts recognize individuals have voluntarily given this information to third parties thereby relinquishing a reasonable expectation of privacy.[21]

B. The Stored Communications Act

The Stored Communications Act (SCA), enacted in 1986, is Title II of the Electronic Communications Privacy Act.[22] The SCA fills in the gaps of the Fourth Amendment to provide more robust privacy protection that the Fourth

---

objects and places, and restrict the government's ability to act beyond the warrant's purview . . . outside of the place identified, which must be described in the document.").

17 *See In re* Search of the Information Associated with [Redacted]@mac.com that is Stored at Premises Controlled by Apple, Inc., 13 F. Supp. 3d 157, 165 (D.D.C. 2014) (illuminating that the search of electronic storage media is not limited to the place where law enforcement executes the search warrant because law enforcement can take the electronic storage media from the place where the warrant is executed and then later search for the stored information that falls within the scope of the warrant).

18 *See* Andrew Guthrie Ferguson, *The "Smart" Fourth Amendment*, 102 CORNELL L. REV. 547, 626 (2017) (explaining that the differences between the protection of the home and an email are the constitutional interests that the courts want to protect).

19 *See* Payton v. New York, 445 U.S. 573, 589 (1980) (asserting that the zone of privacy is nowhere "more clearly defined than when bounded by the unambiguous physical dimensions of an individual's home—a zone that finds its roots in clear and specific constitutional terms."); Groh v. Ramirez, 540 U.S. 551, 557 (2004) (stressing the importance of the particularity requirement); *see also* Kyllo v. United States, 533 U.S. 27, 39 (2001) ("In the home, our cases show, *all* details are intimate details, because the entire area is held safe from prying government eyes.").

20 *See* United States v. Christie, 624 F.3d 558, 573 (3d Cir. 2010) (holding that a plaintiff does not have a reasonable expectation of privacy in its IP address as it is metadata under the Fourth Amendment).

21 Chris Conley, *Non-Content Is Not Non-Sensitive: Moving Beyond the Content/Non-Content Distinction*, 54 SANTA CLARA L. REV. 821, 822–25 (2014); 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, 1210 (2004).

22 18 U.S.C. § 2703(a) (2016); Microsoft II, 829 F.3d 197, 205 (2d Cir. 2016).

Amendment does not expressly provide.[23] Congress enacted the SCA to protect a user's private information, including content[24] and non-content information[25] by imposing regulations primarily on electronic communication service providers[26] and remote computing service providers.[27] The SCA also places limitations on when the government may compel an ISP to disclose stored content and non-content information.[28] More specifically, the SCA protects information in electronic storage such as email and social media messages.[29] The SCA defines "electronic storage" as the "temporary, intermediate storage of a wire or electronic communication . . . and any storage of such communication . . . for purposes of backup protection."[30] Congress enacted the SCA to bolster privacy rights in the user's data held by service providers, protect users from impermissible disclosure by service providers, and set boundaries for the

---

23 Alexander Scolnik, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 350–51 (2009); *see also* S. Rep. No. 90-541, at 5 (1986) (discussing how the "law must advance with the technology" when the Department of Justice recommended amendments to ECPA).

24 William Jeremy Robison, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1207 (2010). Content information includes the substantive information of the email, including the subject line, any components of the message in the email, and attachments. Laura J. Tyson, *A Break in the Internet Privacy Chain: How Law Enforcement Connects Content to Non-Content to Discover an Internet User's Identity*, 40 SETON HALL L. REV. 1257, 1265 (2010).

25 Daniel Shickich, *What Your Tweet Doesn't Say: Twitter, Non-Content Data, and the Stored Communications Act*, 8 WASH. J.L. TECH. & ARTS 457, 459 (2013). Non-content information of an email includes sender and recipient email addresses, time when email was sent and IP addresses. In re § 2703(d), 787 F. Supp. 2d 430, 435 (E.D. Va. 2011); *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 I].

26 18 U.S.C. § 2703(a). Electronic communication service is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications." 18 U.S.C. § 2510(15) (2016).

27 18 U.S.C. § 2703(b) (2016). The SCA defines remote computing service as "provision to the public of computer storage or processing services by means of an electronic communications system." 18 U.S.C. § 2711(2) (2016).

28 18 U.S.C. § 2703 (2016). *See generally* 18 U.S.C. § 2510(15) (defining "electronic communication service providers" as a service which provides to users thereof the ability to send or receive wire or electronic communications); 18 U.S.C. § 2711(2) (defining "remote computing service providers" as entity providing computer storage or processing services by means of an electronic communications system to the public).

29 *Stored Wire and Electronic Communications (Title II of the Electronic Communications Privacy Act—The Stored Communications Act)*, 4 E-COMMERCE AND INTERNET LAW 44.07 (Dec. 2017).

30 18 U.S.C. § 2510(17) (2016); Electronic storage is not the information an individual stores or backs up on his or her hard drive, but rather the information a service provider holds in its capacity as providing services to its users. *Stored Wire and Electronic Communications (Title II of the Electronic Communications Privacy Act—The Stored Communications Act)*, supra note 29.

government when it seeks to compel disclosure of a user's account information from service providers.[31] Together, these statutory privacy rights allow account holders protections similar to those in the Fourth Amendment.[32]

The SCA restricts disclosure by ISPs to third parties with certain limited exceptions set forth in Section 2702 of the SCA ("Section 2702") including, "consent of the originator [sender of the e-mail] or upon notice to the intended recipient, or pursuant to § 2703."[33] Together, Sections 2702 and 2703 are arguably the "heart of the SCA."[34] These provisions permits a governmental entity to compel a service provider to disclose its customers' communications and records subject to a valid warrant, administrative subpoena, grand jury or trial subpoena, or court order.[35]

When required, warrants issued under the SCA by a federal court of competent jurisdiction must be based on probable cause and in compliance with standards set forth in Rule 41 of the Federal Rules of Criminal Procedure, or applicable criminal procedures of states with jurisdiction over the matter.[36] Law enforcement must obtain a warrant for the information an electronic communication service provider stores for 180 days or less under Section 2703(a).[37] If either an electronic communication service provider or a remote computing service provider stores the information for more than 180 days, then the governmental entity does not need a warrant so long as it provides prior notice to the customer.[38]

II. PROCEDURAL BACKGROUND INFORMATION AND THE

---

31 *See* 18 U.S.C. §§ 2701–2703 (2016) (creating causes of action for intentional unauthorized access to, or dissemination of, electronic communications); *see* Kerr, *supra* note 21, at 1213 (stating that 18 U.S.C. § 2702 places limits on situations in which ISPs can voluntarily disclose data to the government).

32 Scolnik, supra note 23, at 372.

33 Microsoft II, 829 F.3d 197, 207 (2d Cir. 2016).

34 Kerr, *supra* note 22, at 1218.

35 Microsoft I, 15 F. Supp. 3d 466, 468–69 (S.D.N.Y. 2014).

36 FED. R. CRIM. P. 41(b)(5)(A)–(C) (governing the procedural rules for law enforcement to be able to search and seize electronic data requiring probable cause by a magistrate judge in federal court); *In re* Search of Information Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *2 (D.D.C. June 2, 2017); Claudia Catalano, Annotation, *Unlawful Access Under Stored Communications Act, 18 U.S.C.A. §§ 2701 et seq.*, 1 A.L.R. Fed. 3d Art. 1 (2015).

37 *Microsoft II*, 829 F.3d at 232.

38 *Id.*; *see* United States v. Scully, 108 F. Supp. 3d 59, 84 (E.D.N.Y. 2015) (holding that failure for the government to provide notice to the account holder is not a violation of the SCA if the government obtains a nondisclosure court order and will not result in an exclusion of evidence).

CURRENT STATE OF COMMON LAW

A. Microsoft I: Magistrate Judge Holding and District Court Holding

Pursuant to a narcotics investigation, the Government served Microsoft Corporation with a warrant under the authority of Section 2703 for content and non-content information associated with a Hotmail account that Microsoft stored.[39] Microsoft moved to quash the warrant on the grounds that it stored some of the requested information, specifically the content information, in Dublin, Ireland.[40] Microsoft argued that the Government's demand for the content-based information stored outside the United States is an impermissible search and seizure under the SCA.[41]

Microsoft based its decision to store such information in Ireland on business grounds and not as a means to hinder law enforcement in connection with their investigation.[42] Microsoft has data centers[43] throughout the United States that stores the content and non-content information associated with each email account.[44] These data centers store the content through a process known as "network latency."[45] Network latency is an automatic process that enables Microsoft to provide efficient service to its customers by storing content at the closest data center.[46] The "country code" determines the closest data center of the account holder when the user registered his or her account.[47] At the end of this process, data centers store all content information outside the United States based on the "country code" of the account holder and some non-content information in the United States.[48]

---

39 *See Microsoft I*, 15 F. Supp. 3d at 467–68 (providing that Microsoft is a United States-based corporation headquartered in Redmond, Washington).

40 *Id.* at 468.

41 *Id.* at 470.

42 Brief for Appellant at 58, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

43 *Microsoft I*, 15 F. Supp. 3d at 467. "A data center is a [physical] repository [where data is stored] that houses computing facilities like servers, routers, switches and firewalls, as well as supporting components like backup equipment, fire suppression facilities and air conditioning*." Data Center*, TECHNOPEDIA, https://www.techopedia.com/definition/349/data-center (last visited May 24, 2018).

44 *Microsoft I*, 15 F. Supp. 3d at 467.

45 *Id*.

46 *Id*.

47 *Id*. A country code is an identification assigned to an email account upon registration. Based on how the end user answers where they are located, Microsoft will assign the country code associated with that country, which determines the appropriate data center. Joint Appendix at 30, United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (No. 17-2), 2017 WL 6206253.

48 *Microsoft I*, 15 F. Supp. 3d at 467.

The magistrate judge addressed whether under the SCA, the Government could compel Microsoft to disclose information even if it stores the information in a foreign country.[49] Examining congressional intent and the structure of the SCA, the judge determined the language regarding compliance with the Federal Rules of Criminal Procedure in Section 2703 to be ambiguous.[50] The ambiguity was whether the judge should incorporate all of Rule 41 or only the procedural requirements.[51] Based on the unique statutory structure of the SCA, the judge determined that warrants issued under the SCA do not act like traditional warrants and resemble a warrant-subpoena hybrid structure.[52] Here, the Government was not entering the premises of the data center owned by Microsoft or searching Microsoft's servers for the requested information.[53] Rather, the Government was compelling Microsoft to provide the requested information under its control.[54]

Further, the judge found the warrant did not raise issues regarding the presumption against extraterritorial application of a statute.[55] The Court held the warrant issued on Microsoft "[did] not criminalize conduct taking place in a foreign country; it [did] not involve the deployment of American law enforcement personnel abroad; [and] it [did] not require even the physical presence of service provider employees at the location where data are stored."[56] It reasoned that the content and non-content information, despite being stored abroad, was at all times under the control of Microsoft in the U.S. and therefore did not induce extraterritorial application issues.[57] The magistrate judge denied

---

49 *Id.* The magistrate judge highlighted the extraterritorial application of the SCA by stating, "[t]he rise of an electronic medium that disregards geographical boundaries throws the law into disarray by creating entirely new phenomena that need to become the subject of clear legal rules but that cannot be governed, satisfactorily, by any current territorially based sovereign." *Id.*

50 *Id.* at 470. Initially, the magistrate judge analyzed the plain statutory language and upon finding Section 2703(a) to be ambiguous whether only procedural rules of 41(a) applied and substantive rules would be encompassed from other sources or whether all of Rule 41 was incorporated by reference. *Id.*

51 FED. R. CRIM. P. 41(d)–(i); *Microsoft I*, 15 F. Supp. 3d at 470.

52 *Microsoft I*, 15 F. Supp. 3d at 471–72. *See generally* Paul K. Ohm, *Parallel-Effect Statutes and E-Mail Warrants: Reframing the Internet Surveillance Debate*, 72 GEO. WASH. L. REV. 1599, 1610–11 (2004) (explaining the hybrid nature between warrants and subpoenas); Orin S. Kerr, *Lifting the Fog of Internet Surveillance: How a Suppression Remedy Would Change Computer Crime Law*, 54 HASTINGS L.J. 805, 815–16 (2002) (explaining that the SCA places restrictions on access to communications and what an ISP can disclose, which is unique to the Fourth Amendment).

53 *Microsoft I*, 15 F. Supp. 3d at 471–72.

54 *Id.* at 476.

55 *Id.* at 475, 477.

56 *Id.* at 475.

57 *Id.* at 477.

Microsoft's motion to quash the warrant.[58] The District Court affirmed the magistrate judge's findings and further held Microsoft in contempt for refusing to comply with the warrant.[59]

B. The Morrison Standard and its Application on Microsoft II

1. Morrison Standard on Extraterritorial Application of Federal Law

The standard for determining extraterritorial application of a federal statute was set forth in *Morrison v. National Australia Bank Ltd*, 561 U.S. 247 (2010).[60] Here, the Supreme Court sought to determine whether Section 10(b) of the Securities Exchange Act of 1934 ("Exchange Act") permitted a foreign plaintiff to file a claim against the United States and foreign defendants for securities traded on a foreign stock exchange.[61] The Supreme Court held that Section 10(b) did not apply extraterritorially.[62] Additionally, it recognized that "the focus of the Exchange Act is not upon the place where the deception originated, but upon purchases and sales of securities in the United States."[63] Justice Scalia wrote the opinion establishing the *Morrison* test and asserted that "[i]t is a longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant to apply only within the territorial jurisdiction of the United States.'"[64] In other words, there is a presumption against extraterritorial application of a federal statute.[65]

In the holding of *Morrison*, the Supreme Court created the proper test for determining extraterritorial application of a statute because prior to this case, there were differentiating tests to which the Circuit and District Courts adhered to, which created impracticable and unpredictable results.[66] The first prong of

---

58 *Id*.

59 *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624, at *1, *5 (S.D.N.Y. Aug. 29, 2014). Tactically, the contempt order allowed Microsoft to appeal without addressing potential jurisdictional issues. Alex Wilhelm, *Microsoft Held In Contempt As It Battles A Domestic Search*, TECHCRUNCH (Sept. 10, 2014), https://techcrunch.com/2014/09/10/microsoft-held-in-contempt-as-it-battles-a-domestic-search-warrant-demanding-overseas-data/.

60 Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 251 (2010).

61 *Id.* at 253 n.2 (citation omitted).

62 *Id.* at 265.

63 *Id.* at 266.

64 *Id.* at 255 (quoting EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)).

65 *Id*.

66 *Id.* at 257; Sec. & Exch. Comm'n v. Berger, 322 F.3d 187, 193 (2d Cir. 2003) (finding the conduct and effect test where jurisdiction only exists if substantial acts that furthered the fraud occurred in the United States), *abrogated by* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).

the *Morrison* test is whether the statute expressly permits extraterritorial application.[67] If the statute does not expressly permit extraterritorial application, then the second prong is to determine the focus of the statute and whether the facts in the case suggest that "the challenged application [will result in an] 'extraterritorial' [application of the law] and [is] therefore outside the statutory bounds."[68]

2. The Application of the Morrison Test in Microsoft II

On appeal, the Second Circuit focused on whether the SCA permits enforcement of warrants outside the United States.[69] The Second Circuit used the *Morrison* two-part test to determine whether a federal statute is intended to apply extraterritorially.[70] The Second Circuit reversed and remanded the District Court's holding in favor of the Government, directing the District Court to quash the part of the warrant compelling disclosure for data stored outside the United States and vacated the District Court's finding of contempt.[71]

Using the *Morrison* test, the Second Circuit found the SCA does not provide for extraterritorial application in Section 2703.[72] Consequently, the SCA failed the first prong of the test.[73] In determining the focus of the statute, the Court analyzed the warrant provision of the SCA.[74] The Court examined the SCA as a whole, the intended contacts of the statute and the legislative history of the SCA.[75] The Court determined the focus of the SCA is to provide user privacy for stored communication as defined in the SCA.[76]

The Court then applied the facts at hand to determine whether such application would result in an impermissible extraterritorial application of the law.[77] Here, the Court noted the citizenship of the individual whose account

---

67 *Morrison*, 561 U.S. at 255; *Regulatory Developments 2012*, 68 BUS. LAW. 843, 971 (2012) (showing that *Morrison* is upheld in higher Circuit Courts).

68 Microsoft II, 829 F.3d 197, 210 (2d Cir. 2016).

69 *Microsoft II*, 829 F.3d at 214–15. Microsoft appealed the District Court's holding, requesting de novo review of the extraterritorial application of the warrant on the grounds that the finding of contempt of court was an "abuse of discretion standard that is more rigorous than usual." Brief for Appellant at 18, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814 (2014) (No. 14-2985-cv).

70 *Microsoft II*, 829 F.3d at 210.

71 *Id.* at 222.

72 *Id.* at 210.

73 *See id.* (disposing of analysis of the *Morrison* test first prong due to Government concession and noting the intended contacts were domestic in nature).

74 *Id.*

75 *Id.* at 211–12.

76 *Id.* at 219.

77 *Id.* at 220.

information the Government sought was not on record—i.e. whether the warrant law enforcement served Microsoft with was for an account holder, who is a citizen of the United States or is a citizen of a foreign country residing outside the United States.[78]

Since the focus of the SCA is user privacy, the Circuit Court found the magistrate judge failed to adequately acknowledge that the user's data at interest is located at a data center in a foreign country. Thus, the Circuit Court found the warrant did not pass the *Morrison* test and that enforcement of the warrant would result in an impermissible extraterritorial application of the SCA.[79] The Second Circuit denied the Government's petition to re-hear the claim *en banc* and subsequently filed a petition for writ of certiorari to the Supreme Court to hear this claim.[80] The Supreme Court granted the petition on October 16, 2017.[81]

C. Potential Circuit Split and District Court Reactions to the *Microsoft* Cases

The Supreme Court's holding may resolve the impending circuit split over the issue of extraterritorial application of Section 2703.[82] In the case, *In re: Information associated with one Yahoo email address that is stored at premises controlled by Yahoo; In re: Two email accounts stored at Google, Inc*., 2017 WL 706307 ((E.D. Wis. Feb. 21, 2017), the court declined to follow the Second Circuit's holding in *Microsoft II*.[83] Just as Microsoft's case, Google and Yahoo stored some of their information in servers outside of the United States on their own accord.[84] The court declined to follow the Second Circuit's decision in *Microsoft II* and provided that the Second Circuit misapplied the *Morrison* analysis.[85] Instead, this court determined the focus of Section 2703 of the SCA is the service provider's obligation to comply with a properly issued warrant and is not user privacy.[86] The District Court ruled in favor of the Government.[87]

The District of Columbia District also declined to follow the Second Circuit's

---

78 *Id*. at 220–21.
79 *Id*.
80 Microsoft v. United States, 855 F.3d 53, 54 (2d Cir. 2017) [hereinafter Microsoft III].
81 Microsoft IV, 138 S. Ct. 356, 356 (2017).
82 18 U.S.C. § 2703 (2016).
83 This is a consolidated case arising out of the warrants issued to Google and Yahoo under 18 U.S.C. § 2703, which compels the disclosure of information as it relates to certain bank accounts. *In re* Information Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307, at *1, *3 (E.D. Wis. Feb. 21, 2017).
84 *Id*. at *1.
85 *Id*. at *2.
86 *Id*. at *3.
87 *Id*. at *1.

holding In The Matter Of The Search of Information Associated with [Redacted] @Gmail.com that is Stored at Premises Controlled by Google, Inc.[88] The magistrate Judge for the D.C. District Court stated the Second Circuit in Microsoft II erred because Google has the ability to access the data stored abroad easily and instantly from the United States.[89] And in this regard, when a judge issues a warrant under the authority of the SCA, thereby compelling a United States-based service provider to disclose certain stored communication, even if the data is stored outside the country, the disclosure would not amount to extraterritorial application of the law.[90] Unlike the Microsoft Court, the D.C. District Court held that the focus of Section 2703 is not user privacy but is disclosure, which constitutes domestic conduct.[91]

III. DISCUSSION

A. The Supreme Court Should Grant the Government's Writ and Should rule in favor of the Government

Under current precedent established by the Supreme Court, requiring a service provider based in the United States to access data stored within the United States is not an impermissible extraterritorially application of Section 2703 of the SCA.[92] To determine whether the application of a law may apply outside the United States, courts turn to a principle of statutory construction that begins with the presumption against extraterritorial application, then resolve this presumption using the two-step process the court established in *Morrison*.[93] This presumption against extraterritoriality "serves to protect against unintended clashes between our laws and those of other nations which could result in international discord."[94] While it is within Congress's powers to enact laws to apply in foreign jurisdictions, determining whether Congress has intended such laws to apply extraterritorially is matter of deduction by the courts.[95] The courts may determine Congressional intent either by looking to the express language

---

88 *In re* Search of Information Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *1, *2 (D.D.C. June 2, 2017).

89 *Id*. at *6.

90 *Id.* at *10.

91 *Id.* at *7, *10.

92 Morrison v. Nat'l Austl. Bank Ltd. 561 U.S. 247, 265 (2010).

93 RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2099 (2016).

94 Kiobel v. Royal Dutch Petroleum Co., 569, U.S. 108, 115 (2013) (quoting EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248 (1991)).

95 U.S. CONST. art. III, § 2, cl. 1; EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 246 (1991), *superseded by statute*, Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1074.

of the statute, the entire related Act or Title as a whole, or whether Congress intended a certain provision to apply outside the confines of the United States.[96]

First, the Supreme Court will look to the express language and legislative history of the statute to rebut the presumption against extraterritoriality. At this step in the analysis, the question is whether the statute itself authorizes application of the law outside the United States.[97] Unless Congress has indicated an intent for foreign application of the law, the presumption is that Congress has legislated over domestic conduct.[98] The Supreme Court has also found permissive extraterritorial application in a statute in which foreign conduct is incidental to the prohibited conduct.[99]

In *Pfizer v. Government of India*, 434 U.S. 306 (1978) the Supreme Court found Congress intended Section 4 of the Clayton Act to include claims brought by foreign nations by examining the legislative purpose of the Act.[100] Distinguishable from *Microsoft II*, the issue in *Pfizer* was whether foreign nations could file a claim for violations of the Sherman Act, and thus maintain the same protections as a domestic corporation or person.[101] The Supreme Court answered in the affirmative, thus effectively allowing applications of the anti-trust protections to apply outside the jurisdiction of the United States.[102]

The Second Circuit found Section 2703 does not expressly authorize extraterritorial application.[103] An examination of the SCA provides that one of Congress' purposes for enacting the SCA was to provide Fourth Amendment-like protections to secured communications by placing obligations on service providers conducting business within the United States from improperly disclosing an individual's data to third parties.[104] The SCA does not purport to authorize enforcement of any of its provisions outside the United States whether by express language or legislative history.[105] The 1986 House Judiciary Committee Report noted the SCA is "intended to apply *only* to access in the

---

96 Arabian Am. Oil Co., 499 U.S. at 265, *superseded by statute*, Civil Rights Act of 1991, Pub. L. No. 102-166, 105 Stat. 1074; *see* Foley Bros. v. Filardo, 336 U.S. 281, 288 (1949) (stating that Congress would not have intended for such an application).

97 *RJR Nabisco*, 136 S. Ct. at 2101.

98 *Id.* at 2100.

99 *See id.* at 2096 (defining "racketeering" to include criminal conduct that impliedly may occur abroad such as the assassination of government agents).

100 15 U.S.C. § 15 (2016); Pfizer, Inc. v. Gov't of India, 434 U.S. 306, 311–12 (1978) (stating that Section 4 of the Clayton Act allowed for any person to file a claim injured by an antitrust violation in a US District Court having jurisdiction over the defendant).

101 *Pfizer*, 434 U.S. at 310–11.

102 *Id.* at 320.

103 Microsoft II, 829 F.3d 197, 210 (2d Cir. 2016).

104 Medina, *supra* note 9, at 276.

105 *Microsoft II*, 829 F.3d at 219.

territorial United States."[106]

The second prong of the *Morrison* test involves determining the focus of the statute.[107] Therefore, the Supreme Court must determine if compelling Microsoft to fully comply with the SCA warrant—even though the content information is located in Ireland—would be an impermissible application of the warrant provision of the SCA.[108] The Court will examine "the 'territorial event[s]' or 'relationship[s]' that are the 'focus'" of Section 2703.[109] If the facts before the court establish sufficient domestic contact, then the presumption against impermissible extraterritorial application will apply and the claim will proceed.[110] In a recent case regarding the application of the *Morrison* test, the Supreme Court acknowledged that at this stage of the analysis, "[the] inquiry into whether the domestic contacts are sufficient to avoid triggering the presumption [against extraterritorial application]."[111]

At the time the Second Circuit decided *Microsoft II*, the Second Circuit was the highest court to consider the issue in *Microsoft II*.[112] However, since then, every other court that has faced the same issue has rejected the Second Circuit's holding.[113] Notably, the Second Circuit is the only court that has found the focus of Section 2703 to be user privacy.[114] The source of discontent among courts is the statutory interpretation of the SCA when determining its focus.[115]

The focus of Section 2703 is the requirement for a service provider based in the United States to comply with a probable cause warrant when the conduct is

---

106 Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 362 (2015) (emphasis added).

107 *Microsoft II*, 829 F.3d at 210.

108 *Microsoft II*, 829 F.3d at 221.

109 Mastafa v. Chevron Corp., 770 F.3d 170, 183 (2d Cir. 2014) (quoting Morrison v. Nat'l Austl. Bank LTD., 561 U.S. 247, 266 (2010)).

110 Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108, 127 (2013).

111 *Microsoft II*, 829 F.3d at 216.

112 *In re* Search of Information Associated with Accounts Identified as [Redacted]@gmail.com and Others Identified in Attachment A that are Stored at Premises Controlled by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA94025, No. 16-mc-80263-RS, 2017 WL 3478809, at *1, *2 (N.D. Cal. Aug. 14, 2017).

113 *In re* Search of Information Associated with [Redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16–mj–757 (GMH), 2017 WL 2480752, at *1, *6 (D.D.C. June 2, 2017); *In re* Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *1, *4 (N.D. Cal. Apr. 25, 2017); *In re* Information Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, Case No. 17-M-1234, 2017 WL 706307, at *1, *3 (E.D. Wis. Feb. 21, 2017).

114 *Microsoft II*, 829 F.3d at 219.

115 *In re* Search of Information Associated with Accounts Identified as [Redacted]@gmail.com and Others Identified in Attachment A that are Stored at Premises Controlled by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94025, No. 16-mc-80263-RS, 2017 WL 3478809, at *1, *2 (N.D. Cal. Aug. 14, 2017).

domestic conduct.[116] Therefore, the location of Microsoft's data centers is irrelevant with regard to the focus of the statute.[117] Accordingly, the Second Circuit was too broad in its review of the focus of the warrant provision of the SCA.[118] When analyzing whether a statute may apply outside the United States, the Supreme Court must concentrate its attention on "the statute provision-by-provision, not as a whole."[119] While Congress enacted the SCA to afford electronic and stored communication protection similar to the Fourth Amendment, it carves out exceptions in the event an electronic service provider is required to disclose information under their control to a government entity.[120]

To emphasize the plain language of the statute, the Government states, the purpose of Section 2703 is to regulate disclosure of private information to the government.[121] This shows that while the SCA as a whole seeks to regulate user privacy by placing obligations on a service provider to prevent unauthorized disclosure to any such third parties, it has expressly allowed law enforcement to compel disclosure of information when the service provider is served with a valid warrant.[122] In accordance with the *Morrison* test, the focus of the Section 2703 is the location of the service provider, who is served with the warrant, not the location of the data center.[123]

If the conduct related to the focus of the statute occurs in the United States rather than abroad, then the application of the statute would be permissible under the *Morrison* test.[124] Therefore, if the focus of the warrant provision of the SCA is the disclosure by the service provider, the location of the service provider and its personnel and the retrieval of the data are all within the United States, which is closer in relation to the focus of the statute.[125] Even though some factors may touch beyond the borders of the United States, such as the location of

---

116 Microsoft II, 829 F.3d at 201(emphasis added).

117 *Id.* at 220.

118 *Id.* at 217.

119 Microsoft III, 855 F.3d 53, 75 (2d Cir. 2017) (Droney, J., dissenting); *see also* United States v. Ballestas, 795 F.3d 138, 144 (D.C. Cir. 2015) (providing that if a provision reaches application abroad, the extraterritorial application will be limited to that one provision and not the whole statute).

120 *Microsoft II*, 829 F.3d at 217.

121 *Id.*

122 *See id.* at 219 (stating that the main reason Congress enacted the SCA was to protect disclosure of content by third-parties and that the warrant requirement of the Fourth Amendment would protect consumers from improper governmental access).

123 *Id.* at 201.

124 *In re* Search of Information Associated with Accounts Identified as [Redacted]@gmail.com and Others Identified in Attachment A that are Stored at Premises Controlled by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94025, No. 16-mc-80263-RS, 2017 WL 3478809, at *1, *2 (N.D. Cal. Aug. 14, 2017).

125 *Id.*

Microsoft's data centers, this factor in particular is not the focus of Section 2703.[126]

After determining the focus of the statute, the facts of the case will be applied to ascertain whether the "challenged application" would result in impermissible extraterritorial application.[127] Requiring Microsoft to comply with the Government's valid warrant would not be an impermissible extraterritorial application of Section 2703.[128] Judge Dennis Jacobs, a Second Circuit judge, noted in his dissent against the denial of the government's rehearing *en banc* that the warrant would not result in unlawful extraterritorial application because the information requested in the warrant related to a Microsoft account holder is "served on Microsoft" and because "[the corporation] has access to the information sought. It need only touch some keys in Redmond, Washington."[129] The act of disclosure is domestic conduct to which Microsoft has access and over which it has control.[130] The location of the data center, whether in the United States or in Ireland, is irrelevant.[131]

B. User Privacy as it Relates to the Fourth Amendment

The central Fourth Amendment implication in the Microsoft case is whether compliance with the warrant issued to Microsoft, under the authority of the SCA, would be a violation of Fourth Amendment protections of its users.[132] Notably, the dissenting opinion denying the Government's rehearing *en banc* articulated that ruling in favor of Microsoft is by no means a victory in protecting user privacy.[133] Following the District Court's decision that ruled in favor of the United States, Microsoft's General Counsel, Brad Smith, claimed that the United States is attempting to "sidestep" the Fourth Amendment.[134] Interestingly, it is Microsoft's argument that "sidesteps" the fact that it, alongside other service providers in the United States, such as Google and Yahoo, automatically store

---

126 *Id.* at *3.

127 Microsoft II, 829 F.3d 197, 210 (2d Cir. 2016).

128 *See id.* (reiterating the presumption that congressional legislation only applies to territorial jurisdiction of the United States).

129 Microsoft III, 855 F.3d 53, 61 (2d Cir. 2017).

130 *See* Jara v. Nunez, 878 F.3d 1268, 1273 (11th Cir. 2018) (providing that an act will be consider domestic if a sufficient amount of relevant contacts is in the United States); *Microsoft III*, 855 F.3d at 61.

131 *Microsoft III*, 855 F.3d at 61.

132 *Id.* at 56.

133 *Id.* at 61.

134 Christopher Boehning & Daniel J. Toal, *Microsoft Paves the Way for Data Privacy*, N.Y. L. J. (Oct. 7, 2014), https://www.law.com/newyorklawjournal/almID/1202672465322/?slreturn=20180006125452.

emails and other data outside the United States as a business decision to improve the productivity of their systems.[135] Thus, the primary motivation of service providers is not to store their data for purposes of stringent user privacy protection.[136]

It is significant to note that Congress enacted the SCA to obligate service providers to protect customers' and subscribers' privacy from the government *and* other third parties.[137] Section 2703 of the SCA is an important focal point when examining the Fourth Amendment-like protections granted to a user's stored communications.[138] Section 2703 "sets up a pyramidal structure governing conditions under which service providers must disclose stored communications to the government."[139] Each ascending tier of the pyramid delineates an increasingly thorough legal process that the government must accomplish before compelling disclosure.[140] The two factors that influence compelling disclosure include (1) whether the data is content or non-content information and (2) whether the issuer provided the user with notice.[141]

The Supreme Court has repeatedly upheld that citizens can reasonably expect less privacy in stored communication, such as emails, because the user relays stored communications to third parties as in line with the reasoning to which the court adhered in *Katz v. United States*, 389 U.S. 347 (1967).[142] When a judge

---

135 Microsoft II, 829 F.3d 197, 203 (2d Cir. 2016). Google has seven data servers located outside of the United States in Chile, Taiwan, Singapore, Ireland, Netherlands, Finland, and Belgium, that provide infrastructure support to their operations. *Data Center Locations*, GOOGLE DATA CENTERS, https://www.google.com/about/datacenters/inside/locations/index.html (last visited May 24, 2018); Charlie Savage, Claire Cain Miller & Nicole Perlroth., *N.S.A. Said to Tap Google and Yahoo Abroad*, N.Y. TIMES, Oct. 31, 2013, at B1.

136 *Microsoft II*, 829 F.3d at 224; *see How Email Works*, RUNBOX, https://runbox.com/email-school/how-email-works/ (last visited May 24, 2018) (describing that in exchange for providing free email services, large email service providers such as Google sell a user's information to certain advertisers based on the content of that user's emails).

137 *Microsoft II*, 829 F.3d at 217; *see also Court Seems Unconvinced Of Microsoft's Argument To Shield Email Data Stored Overseas*, NPR (Feb. 27, 2018 5:00 AM), https://www.npr.org/2018/02/27/584650612/new-front-in-data-privacy-at-the-supreme-court-can-u-s-seize-emails-stored-abroad (noting that the Fourth Amendment does not expressly provide protection in data stored by a third party and protection on such data has been by convention of common law and the SCA).

138 *Microsoft II*, 829 F.3d at 207; *see* Rudolph J. Burshnic, *Applying the Stored Communications Act to the Civil Discovery of Social Networking Sites*, 69 WASH. & LEE L. REV. 1259, 1261–62 (2012) (stating that the SCA provides "Fourth Amendment plus" protection to communication stored by a statutorily defined service provider).

139 *Microsoft II*, 829 F.3d at 207.

140 *Id.*

141 *Id.*; Kattan, *supra* note 16, at 629–30.

142 *See* United States v. Jones, 565 U.S. 400, 417 (2012) (finding that a person has no

issues a warrant under the SCA based on probable cause and in accordance with applicable Federal Rules of Criminal Procedure, the warrant is presumptively constitutionally valid and has provided the necessary deference by law enforcement to respect the individual's privacy.[143] Regarding the warrant served on Microsoft, the dissenting judges in the denial of a rehearing *en banc* reiterated that "the government complied with the most restrictive privacy-protecting requirements of the [SCA]. Those requirements are consistent with the highest levels of protection ordinarily required by the fourth Amendment for the issuance of search warrants."[144] It is integral to consider that the underlying reason that prompted the SCA's enactment was the courts grappling with how they should treat electronic communications under the Fourth Amendment.[145]

C. Conflicts of Law Analysis and the Implications of Ruling in Favor of Microsoft as it Relates to International Comity

Given the nature of data transfers, *Microsoft v. United States* is a cross-border case implicating the laws of the United States, EU, Ireland the state where the account holder is located.[146] To understand the ramifications of a decision, which rules in favor of Microsoft, a review of Brainerd Currie's "interest analysis" for conflicts of law issues, otherwise known as "governmental interest analysis," is appropriate to determine whether there is in fact a conflict and whose law should apply.[147] The first step is to determine each jurisdiction's

---

expectation of privacy in information disclosed to a third party); Katz v. United States, 389 U.S. 347, 351 (1967) (finding that the Fourth Amendment protects people, not places, so "[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection."); s*ee also* Smith v. Maryland, 442 U.S. 735, 742 (1979) (holding that use of a pen register to record phone numbers does not constitute a search when the information has been disclosed to a third party because there is no reasonable expectation of privacy).

143 Kerr, *supra* note 21, at 1209 (2004).

144 Microsoft III, 855 F.3d 53, 63 n.5 (2d Cir. 2017) (Cabranes, J., dissenting) (quoting Microsoft II, 829 F.3d 197, 223 (2d Cir. 2016)) (Lynch, J., concurring).

145 *Microsoft II*, 829 F.3d at 219.

146 *Id.* at 230.

147 *See* Budget Rent-A-Car Sys., Inc. v. Chappell, 407 F.3d 166, 170 (3d Cir. 2005) (holding if a case presents a true conflict among multiple jurisdictions, then the country that has the most significant contacts or relationships with issue would apply). In the *Microsoft* case, by counting substantial contacts in the facts, federal law could apply given that Ireland and the EU's only contact with the case is that the data center is located in Ireland and all other relevant contacts are located in the United States. *See* Bruce Posnak, *Choice of Law: Interest Analysis and Its "New Crits"*, 36 AM. J. COMP. L. 681, 686–89 (1988) (describing when to use the governmental interest analysis); BRAINERD CURRIE, SELECTED ESSAYS ON THE CONFLICTS OF LAWS 52–53 (1963); *see also* Andrew D. Bradt, *Resolving Intrastate Conflicts of Laws: The Example of the Federal Arbitration Act*, 92 WASH. U.L. REV. 603, 607 (2015).

policy behind the conflicting laws at issue.[148] The next step is to determine whether the jurisdiction in fact has an interest in the application of its laws.[149]

Currie based his interest analysis theory on the premise that legislatures create laws to serve social goals.[150] When deciding upon choice-of-law, Currie argued that the governmental interests of each interested jurisdiction should have deference in having its law govern a claim or issue.[151] Currie's interest analysis seeks to provide guidance to the courts to apply the law of a sovereign that would further its policy goal.[152] An interest analysis, applied to the issues raised in the *Microsoft* cases, would effectively address whether a false conflict or true conflict exists between the EU and the United States.[153] A "false conflict" exists where applying only one country's laws would achieve the policy goals, in which case the court is to apply that country's laws.[154] A "true conflict" is when the application of a set of laws furthers each jurisdiction's policies. In this case, the court is to apply forum law, find a "middle ground" interpretation of one of the countries to avoid disruption in comity among the interested nations or, in the alternative, apply the law of the jurisdiction whose policies would be comparatively impaired.[155]

A conflicts analysis of the *Microsoft* cases centers upon the warrants issued

---

148 Bradt, *supra* note 147, at 613; *see also* Brainerd Currie, *Notes on Methods and Objectives in the Conflict of Laws*, 1959 DUKE L.J., 171, 178 (1959) (describing a basic, yet comprehensive approach to applying Currie's interest analysis).

149 Bradt, *supra* note 147, at 613.

150 *Id.* at 612; *see also* CURRIE, *supra* note147, at 52, 70.

151 Bradt, *supra* note 147, at 616; Brainerd Currie, *Married Women's Contracts: A Study in Conflict-of-Laws Method*, 25 U. CHI. L. REV. 227, 261 (1958).

152 Bradt, *supra* note 147, at 613–615; Currie, *supra* note 151, at 261. Currie argued a jurisdiction's law represents a policy decision of the legislature. When the laws of multiple jurisdictions are applicable to a claim, then implicitly each state or country may have an interest in its law applying to further its policy goals. Alfred Hill, *The Judicial Function in Choice of Law*, 85 COLUM. L. REV. 1585, 1589 (1985).

153 *See* Budget Rent-A-Car Sys., Inc. v. Chappell, 407 F.3d 166 (3d Cir. 2005) (providing the most significant relationship test to perform a conflicts of law analysis is where a true conflict exits). The Court held if a case presents a true conflict among multiple jurisdictions, then the country that has the most significant contacts or relationships with issue would apply. *Id.* In the case of Microsoft, by counting substantial contacts in the facts, federal law could apply given that Ireland and the EU's only contact with the case is that the data center is located in Ireland and all other relevant contacts are located in the United States. Bradt, *supra* note 147, at 615, 617. For an overview of how to apply Currie's interest analysis, *see* WILLIAM RICHMAN, WILLIAM REYNOLDS, & CHRISTOPHER WHYTOCK, UNDERSTANDING CONFLICTS OF LAWS 253–54 (4th ed. 2013).

154 Bradt, *supra* note 147, at 615; *see also* Currie, *supra* note 151, at 251–52 (stating "these are the cases in which application of the law of the place of making advances the interest of one state without impairing any interest of the other.").

155 Bradt, *supra* note 147, at 616; RICHMAN ET AL., *supra* note 153, at 260–262; Herma Hill Kay, *The Use of Comparative Impairment to Resolve True Conflicts, An Evaluation of the California Experience*, 68 CALIF. L. REV. 577, 579–80 (1980).

under Section 2703 of the SCA to a United States based email service provider.[156] Enforcement of the warrant implicates foreign interests narrowly because Microsoft's data center is stored in Ireland, a Member State of the EU, and broadly because of the prevalence of data centers in foreign countries operated by service providers headquartered in the United States.[157] The interested contacts to consider under the conflicts of law analysis are: (1) the user whose account information the government is requesting, (2) Microsoft[158], (3) the United States, (4) Ireland, and (5) the European Union.[159]

The United States has an interest in the enforcement of the warrant served on Microsoft to allow for law enforcement to efficiently investigate crimes. Given the prevalence of the use of email communication, the content of emails are a vital part of law enforcement's investigations.[160] Under these circumstances, when a crime is committed in violation of federal or state law in the United States; by convention, the location in which the evidence of the crime is stored by a third party that is independent of such investigation, does not advance or achieve societal interest when balanced against user privacy.[161] Given the government's interest in user privacy and the investigation of cybercrimes, when

---

156 Microsoft I, 15 F. Supp. 3d 466, 467–68 (S.D.N.Y. 2014).

157 Microsoft II, 829 F.3d 197, 203 (2d Cir. 2016); *see* Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament Supporting Appellant at 6, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985-cv); *see also* Pablo Valerio, *US Firms Looking to Europe for Data Protection*, NETWORK COMPUTING (May 26, 2016), https://www.networkcomputing.com/cloud-infrastructure/us-firms-looking-europe-data-protection/129277031 (stating that many large internet companies including Microsoft, Apple, Facebook, and Google have recently been building large data centers in Europe).

158 *See Court Seems Unconvinced Of Microsoft's Argument To Shield Email Data Stored Overseas*, *supra* note 137 (providing that Microsoft's concern in the enforcement of the warrant is that other foreign countries would not go through the proper federal channels to obtain data stored in the United States and would start a "global free-for-all.").

159 Posnak, *supra* note 147, at 686–89; *Microsoft Services Agreement*, MICROSOFT (July 15, 2016), https://www.microsoft.com/en-US/servicesagreement/ ("[T]he laws of the state where [the user] live[s] govern[s] all claims, regardless of conflict of laws principles."). The interest of the account holder thus would be implicated when they would have claims or remedies available to them under applicable state privacy laws depending upon where the user resides when the privacy violation, if any, occurred. *Id.*

160 *See* Brief for the States of Vermont, Alabama, Arizona, Arkansas, Connecticut, Delaware, Hawaii, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maine, Maryland, Massachusetts, Michigan, Montana, Nebraska, New Hampshire, New Mexico, New York, North Carolina, Ohio, Oregon, Pennsylvania, South Carolina, South Dakota, Texas, Utah, Virginia, Wyoming and the Commonwealth of Puerto Rico as Amici Curiae in support of petitioner at 7–8, Microsoft IV, 138 S. Ct. 356 (2017) (No. 17-2) [hereinafter Brief for States] (providing that crimes involving the exploitation of children – including child pornography, luring minor children, kidnapping, etc., – often require law enforcement to issue probable cause warrants for information stored in emails and instant messaging communications); Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HARV. L. REV. 531, 532 (2005).

161 Brief for States at 7–8, Microsoft IV, 138 S. Ct. 356 (2017) (No. 17-2).

there is probable cause and a magistrate judge issues a valid warrant, the government meets its burden to compel the service provider to disclose the requested information consistent with the requirements of the SCA.[162]

Whereas, the EU considers privacy to be a human right; and the EU considers data protection to be a fundamental right.[163] The EU also has a significant interest in protecting their citizen's privacy when their citizens have created an email account with a United States-based service provider.[164] Accordingly, the EU's privacy regulations subject all personal data stored in its countries to the most stringent standards to protect the autonomy of the account holder.[165] The EU's enacted several directives, including the Data Protection Directive[166] and the ePrivacy Directive,[167] to further its interest in protecting the privacy of its citizens and harmonize data security laws across the board to ensure comprehensive protection internationally.[168] These privacy protection laws are currently provided in Directive (EU) 2016/680, which came into effect on May 5, 2016.[169]

While the laws regarding privacy protection are specifically enumerated in the Directive, the EU Charter on Fundamental Rights considers the protection of personal data and privacy of individuals as a fundamental human right.[170] The EU curated the Charter and the Directive to balance the importance of the need to protect the integrity and dignity of its citizens with the free flow of data, while creating exceptions that allow law enforcement to conduct authorized activities for the purposes of national security and safety of its citizens.[171] Collectively,

---

162 Microsoft II, 829 F.3d 197, 223 (2d Cir. 2016).

163 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 6–7, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

164 *Id.*; *see also* Julia M. Fromholz, *The European Union Data Privacy Directive*, 15 BERKELEY TECH. L.J. 461, 461–62, 466–69 (2000).

165 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 4, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

166 Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC). This Directive governs the processing and transfer of personal data stored in the EU and was adopted by the EU Member States. *Id.*

167 Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC). This Directive supplements the Data Protection Directive by providing specific obligations on service providers to safeguard electronic communications and restrict access of the communications for purposes of providing the services. *Id.*

168 Fromholz, *supra* note 164, at 466, 468, 470.

169 Parliament and Council Directive 2016/59, 2016 O.J. (L119)(EC); The EU originally enacted this Directive in 2002 and the ePrivacy Directive later supplemented it in 2002. Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC). Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC).

170 Charter on Fundamental Rights of the European Union, art. 8, Mar. 30, 2010, 2010 O.J. (C83) 389; Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

171 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament

the EU privacy protection laws provide, "personal data can only be gathered legally under strict conditions, for a legitimate purpose."[172] In enacting its laws, the EU recognizes that individuals and organizations – both public and private – transfer data across borders.[173] Despite conflicting laws of other countries, the EU strives to unilaterally protect all data within the jurisdiction of the EU to the most stringent standards by regulating the transfer of data containing personal information outside the EU.[174]

The EU has dedicated a significant amount of its resources to various EU agencies and officials to oversee and enforce data protection and privacy concerns of individuals.[175] Data Protection Authorities ("DPAs") in each member state of the European Union, including Ireland, ensure that each individual's privacy rights are in compliance with the applicable privacy laws.[176] If an entity violates a citizen's privacy rights, then he or she may file complaints with DPAs and cease a data controller's prohibited actions.[177] The European Data Protection Supervisor ("EDPS") is a dedicated independent agency that governs and oversees the processing of personal data to ensure compliance with the Directive.[178] The main roles of the EDPS are to supervise controllers of

---

supporting Appellant at 7, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31, Note 8 (EC); *see also* Parliament and Council Directive 2002/58, 2002 O.J. (L 201) 37 (EC); *see also* Parliament and Council Directive 95/46, 1995 O.J. (L 281) 31, 39 (EC).

172 *Protection of personal data*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/ (last visited May 24, 2018).

173 *Id.*

174 *Id.*; *see also* William Bruce Wray, *A European Approach to the United States Constitutional Privacy*, 5 CREIGHTON INT'L & COMP. L.J. 51, 61 (2014) (stating European law outlines a set of rights and principle for the treatment of personal data, whereas U.S. law does not).

175 For a full list of administrative bodies and data protection authorities in the U.N., *see Data Protection Bodies*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/bodies/index_en.htm. For a general discussion of the statutory foundations of data protection authorities and their role in the regulation of data protection in the European Union, *see* Francoise Gilbert, *Proposed EU Data Protection Regulation: The Good, The Bad, and the Unknown*, 15 No. 10 J. INTERNET L. 1, 21, 31–32 (2012).

176 FACT SHEET: OVERVIEW OF THE EU-U.S. PRIVACY SHIELD FRAMEWORK, https://www.commerce.gov/news/fact-sheets/2016/02/fact-sheet-overview-eu-us-privacy-shield-framework (last visited May 24, 2018).

177 DEP'T OF COMM., FACT SHEET: OVERVIEW OF THE EU-U.S. PRIVACY SHIELD FRAMEWORK (Feb. 29, 2016), https://www.commerce.gov/sites/commerce.gov/files/media/files/2016/eu-us_privacy_shield_fact_sheet.pdf; *see* Virginia Boyd, *Financial Privacy in the United States and the European Union: A Path to Transatlantic Regulatory Harmonization*, 24 BERKELEY J. INT'L L. 939, 984 (2006) (explaining while individuals can "receive support and redress," penalties "are rarely used because compliance can be achieved through negotiation and consultation with the DPA.").

178 Ryan Moshell, *And Then There Was One: The Outlook for A Self-Regulatory United States Amidst a Global Trend Toward Comprehensive Data Protection*, 37 TEX. TECH L.

personal data, provide consultation to legislators, and to ensure cooperation with other data protection authorities.[179]

There are significant differences between the privacy laws of the EU and the United States.[180] A legal scholar on transnational law summarized the major differences between privacy protection in the United States and in the EU regarding data flow between the two countries.[181] First, the presumption of disclosing data by a commercial service provider in the United States is de facto permitted unless a statute expressly prohibits it.[182] Second, the EU prohibits the disclosure of data to third parties unless the law expressly permits it.[183] In the United States, an individual may waive his or her privacy rights by contract, such as those in click-wrap agreements when signing up for a user account.[184] Contrastingly, the EU does not enforce these agreements against a user and the EU imposes far greater restrictions on service providers to protect a user from unknowingly waiving his or her rights away.[185] Regardless, it is important to

---

REV. 357, 369 (2005); *see* EUROPEAN DATA PROT. SUPERVISOR, https://edps.europa.eu/about-edps_en (last visited May 24, 2018) (striving to enforce and reinforce EU data protection and privacy standards, both in practice and law).

179 Moshell, *supra* note 178, at 369.

180 Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1, 22 (2000) (referring to EU data privacy regulation as centralized as compared to the United States which is described as "narrowly targeted to specific sectors" and "uncoordinated"); *see also* David Lazarus, *Europe and U.S. have different approaches to protecting privacy of personal data*, L.A. TIMES (Dec. 22, 2015), http://www.latimes.com/business/la-fi-lazarus-20151222-column.html (stating how the European Union begins with the understanding that privacy is a human right as opposed to how the United States begins with the understanding of how privacy will affect business); Mark Scott & Natasha Singer, *How Europe Protects Your Online Data Differently Than the U.S.*, N.Y. TIMES (Jan. 31, 2016), https://www.nytimes.com/interactive/2016/01/29/technology/data-privacy-policy-us-europe.html?smid=pl-share (explaining how, under the European privacy laws, individuals can request companies to provide "details about what data it holds" and "what the information is used for;" however, under the U.S. privacy laws, "[t]here is no single federal law or standard people can rely on to obtain copies of their records.").

181 The guidance was provided by Professor Ioanna Tourkochoriti of Harvard University. Ioanna Tourkochoriti, *The Snowden Revelations, the Transatlantic Trade and Investment Partnership and the Divide Between U.S.-EU in Data Privacy Protection*, 36 UALR L. REV. 161, 164 (2014).

182 *Id.* at 164; *see also* 5 Leslie T. Thornton & Edward R. McNicholas, SUCCESSFUL PARTNERING BETWEEN INSIDE AND OUTSIDE COUNSEL § 82:47, EU Data Protection Law (2017) (explaining how the Directive's adoption of preventing the commercial use of an individual's data without consent has had an impact on United States' businesses).

183 Tourkochoriti, *supra* note 181, at 164.

184 Jennifer L. Bauer, *Playing Off-Key: Trans-Atlantic Data Regulation in A Discordant World*, 119 W. VA. L. REV. 793, 799 (2016); *see, e.g.*, Julie E. Cohen, *DRM and Privacy*, 18 BERKELEY TECH. L.J. 573, 605 (2003) (explaining how adhesion contracts waive privacy rights but there are issues with consent).

185 Bauer, *supra* note 184, at 799; *see also Guidelines in relation to legal basis for*

note that a data service provider is required to provide notice to a user prior to disclosure of the user's information to a third-party if disclosure is not related to a legitimate purpose.[186]

Third, the EU provides broader protection to the user than the United States provides to the user.[187] The EU provides very limited instances where a service provider may disclose personal data.[188] When a privacy right conflicts with another right of an individual, the former is likely to prevail because privacy and confidentiality are considered fundamental rights.[189] However, in the United States, the Bill of Rights specifically enumerates that other rights will outweigh privacy concerns in data because they are often considered secondary to those enumerated in the United States Constitution.[190] The Directive defines "Personal data" as "any information relating to an . . . identifiable natural person [and] an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity."[191] The United States lacks any statutory or concise common law definition of personal data.[192]

The EU has an independent agency specifically designed to enforce the privacy laws in the Directive.[193] But the United States does not have even one federal enforcement agency that oversees privacy regulations.[194] Rather, there are staff members and Inspector-Generals within the various law enforcement agencies that ensure other agencies are complying with applicable statutes.[195]

---

private sector sharing of personal data, DATA PROT. COMM'R (Mar. 14, 2018), https://www.dataprotection.ie/docs/Commissioner-launches-new-guidance-on-data-sharing-in-the-private-sector/530.htm ("Where this consent is sought as a condition for the provision of the service . . . it is doubtful that it can be considered to be freely given and therefore should not normally be solely relied upon as a justification for the sharing of personal data.").

186 Tourkochoriti, *supra* note 181, at 164.

187 *Id.*

188 § 82:47 EU data protection standards—Choosing international transfer compliance options—Safe harbor, 5 Successful Partnering Between Inside and Outside Counsel § 82:47.

189 Tourkochoriti, *supra* note 181, at 164.

190 *Id.*; *see also* Bartnicki v. Vopper, 532 U.S. 514, 534 (holding the First Amendment's right to freedom of speech will take priority over the Fourth Amendment where the released information is a matter of public concern).

191 Tourkochoriti, *supra* note 181, at 168 (quoting Council Directive 95/46/EC of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281) 25).

192 *See* Tourkochoriti, *supra* note 181, at 168; Bauer, *supra* note184, at 799 (providing that personally identifiable information subject to privacy regulations is recognized as two pieces of information in a database that can directly identify an individual).

193 Bauer, *supra* note 184, at 799.

194 Opinion 01/2016 on the EU – U.S. Privacy Shield Draft Adequacy Decision, Eur. Parl. Doc., WP 238 (2016).

195 *Id.*

These agencies are not solely dedicated to overseeing compliance with privacy regulations.[196]

Article 4 of Directive provides that the law of the Member State where the data is processed shall apply.[197] In this instance, Microsoft's data center in Ireland would be governed by Ireland's laws and enforced by the Data Protection Act in Ireland. The Data Protection Act of 1988 governs Ireland's data privacy laws, and the Data Protection (Amendment) Act of 2003 amended it, (together the "Data Protection Act").[198] The DPA encompasses the privacy laws in the Directive, including the obligation of ISPs storing and processing personal data to comply with these regulations.[199] Microsoft's maintenance and control over its data centers in Ireland thereby requires it to comply with both the Directive and Ireland's statutory law.

Under the circumstances of the *Microsoft* cases, Ireland's DPA may conclude the user of the email account has not consented to the processing of his or her data.[200] The Directive provides consent must be "freely given, specific, informed and unambiguous."[201] Under the Irish DPA, consent would be deemed

---

196 *Article 29 Working Party in the Opinion 01/2016 on the EU-U.S. Privacy Shield draft adequacy decision*, at 40, (Apr. 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2016/wp238_en.pdf. The Federal Trade Commission ("FTC") is responsible for enforcing regulations to protect the privacy of consumers but the FTC is not solely dedicated to enforcing privacy regulations. Alan Charles Raul, Frances E. Faircloth & Vivek K. Mohan, *United States*, *in* THE PRIVACY, DATA PROTECTION AND CYBERSECURITY LAW REVIEW 365 (Alan Charles Raul ed., 4th ed. 2014).

197 Art. 4(1)(a), Directive 95/46/EC.

> Each Member State shall apply the national provisions it adopts pursuant to this Directive to the processing of personal data where: (a) the processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State; when the same controller is established on the territory of several Member States, he must take the necessary measures to ensure that each of these establishments complies with the obligations laid down by the national law applicable.

Id.

198 Data Protection Acts 2003 (Ir.); Data Protection Acts 1988 (Ir.).

199 Data Protection Acts 2003 (Ir.); Robert Clark, *Data Protection in the Republic of Ireland*, 11 INT'L REV. L. COMPUTERS & TECH. 203, 203 (1997).

200 Member States shall provide that personal data may be processed only if the data subject has unambiguously given his consent, Article 7(a), Directive 95/46/EC; *see also* Lee Matheson, *European Commission Weighs in on Microsoft Ireland Case*, IAPP (Dec. 17, 2017), https://iapp.org/news/a/european-commission-weighs-in-on-microsoft-ireland-case/ (providing that disclosure to the United States from Ireland of the requested information under the warrant issued to Microsoft would qualify as processing under the Directive).

201 Art. 4(11)(a), Directive 95/46/EC; *see also Consent as a Legal Basis for Processing Data*, WHITNEY MOORE (Jan. 2018), http://whitneymoore.ie/2018/01/25/consent-legal-basis-processing-data/.

unlikely when it is provided as a condition to open an email account with Microsoft through the click-wrap terms and conditions.[202] Microsoft's Master Service Agreement, which governs the use of its email services, is silent on disclosure to third parties.[203] It is unlikely that the failure to provide language regarding disclosure to third parties or the safeguarding of the user's data would pass muster under Irish law. Ireland has a sufficient interest in its laws applied to the transferring of data from the data center in Ireland to the United States because Microsoft could be found in violation of the Directive for complying with warrant issued by the United States.[204]

These distinct differences in privacy protection have historically been a point of contention between the EU, Ireland, and the United States.[205] In 2000, as a means to alleviate the differences in international privacy policy, the EU and the United States entered into the now invalidated, Safe Harbor Privacy Principles.[206] The United States Department of Commerce and the EU negotiated a series of principles to govern data flow from the EU to the United States to ensure compliance with the stringent privacy regulations in the Directive.[207] If a company regulated either by the United States Department of Commerce or by the Federal Trade Commission complied with the principles set forth in the Safe Harbor arrangement, then the presumption was that it complied with the Directive allowing for companies to transfer data from the EU to the United States without prior approval.[208]

---

202 Expert Report and Affidavit for Respondent at 5, Federal Trade Commission v. The Western Union Co., 2013 WL 12107385 (S.D.N.Y. 2013) ("[W]here this consent is sought as a condition for the provision of the service in question rather than on a purely optional basis, the strong view of the Commissioner is that it is doubtful that it can be considered to be freely given and therefore should not normally be solely relied upon as a justification for sharing personal data.").

203 *Master Services Agreement*, MICROSOFT (July 15, 2016), https://www.microsoft.com/en-US/servicesagreement/.

204 *See* Expert Report and Affidavit for Respondent at 5, Federal Trade Commission v. The Western Union Co., 2013 WL 12107385 (S.D.N.Y. 2013) (noting that in a case involving the transfer of data from a Western Union processing data in Ireland to the United States, Western Union could be subject to penalties for violation of the Directive).

205 Federico Fabbrini, *Human Rights in the Digital Age: The European Court of Justice Ruling in the Data Retention Case and Its Lessons for Privacy and Surveillance in the United States*, 28 HARV. HUM. RTS. J. 65, 90 (2015).

206 U.S. DEP'T OF COMMERCE, U.S.-EU SAFE HARBOR FRAMEWORK A GUIDE TO SELF-CERTIFICATION 10 (Mar. 2009), https://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf.

207 Christopher Wolf, Safe Harbors for U.S./eu Personal Data Transfers, Prac. Law., April 2001, at 13.

208 Robert R. Schriver, *You Cheated, You Lied: The Safe Harbor Agreement and Its Enforcement by the Federal Trade Commission*, 70 FORDHAM L. REV. 2777, 2780 (2002); *see also* U.S. DEP'T OF COMMERCE, U.S.-EU SAFE HARBOR FRAMEWORK A GUIDE TO SELF-CERTIFICATION 11 (Mar. 2009), https://www.trade.gov/publications/pdfs/safeharbor-selfcert2009.pdf (providing that to obtain the benefits of the Safe Harbor arrangement,

In 2015, the Court of Justice of the European Union invalidated the Safe Harbor Privacy Principles significantly impacting companies that receive data from the EU in *Schrems v. Data Protection Commissioner*.[209] The case involved an Austrian citizen who filed a claim with the Irish Data Protection Commissioner on the grounds that Facebook's transfer of his data outside the EU failed to comply with the Directive.[210] The Irish High Court referred the case to the Court of Justice of the European Union, the EU's highest court, to resolve the issue of whether it should ban data transfers from the EU to the United States.[211] The Court of Justice of the European Union found that in transferring personal data from the EU to the United States, the United States, "lacked[ed] adequate protection of personal data" and nullified the presumption of United States compliance with the Directive established in the Safe Harbor Principles.[212] The invalidation of the Safe Harbor Principles provided evidence to the EU that data transfers between the EU and the United States would not be in compliance with the directives of the Safe Harbor Principles.[213]

Currently, the United States has Mutual Legal Assistance Treaties ("MLATs") with certain countries, which allows the United States to formally

---

companies had to abide by principles of the Safe Harbor, including maintaining reasonable security measure to protect the integrity of the data and providing notice to individuals when transferring their data to a third party).

209 Christina Lam, *Unsafe Harbor: The European Union's Demand for Heightened Data Privacy Standards in Schrems v. Irish Data Protection Commissioner*, 40 B.C. INT'L & COMP. L. REV. 1, 6 (2017).

210 *Id.* at 4; Maximilian Schrems, *Complaint against Facebook Ireland Ltd – 23 "PRISM"*, EUROPE V. FACEBOOK 1, 3 (June 25, 2013), http://www.europe-v-facebook.org/prism/facebook.pdf; *see* Conor Humphries, *Ireland asks Europe's top court to rule on EU-U.S. data transfers*, REUTERS (Oct. 3, 2017, 6:30 AM), https://www.reuters.com/article/us-eu-privacy-facebook/ireland-asks-europes-top-court-to-rule-on-eu-u-s-data-transfers-idUSKCN1C80XQ (stating that Maximilian Schrems alleges that Facebook transferred his personal data outside of the EU and failed to comply with the Directive); *see also* Thomas Fox-Brewster, *'Landmark' Decision Threatens Facebook Use of European Personal Data*, FORBES (Oct. 6, 2015, 4:58 AM), https://www.forbes.com/sites/thomasbrewster/2015/10/06/safe-harbour-invalid/#3f6fe42c1d98 (describing the initial complaint and case filed against Facebook).

211 Humphries, *supra* note 210.

212 Fox-Brewster, *supra* note 210; Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R. 650; Court of Justice of the European Union Press Release No. 117/15, The Court of Justice declares that the Commission's US Safe Harbour Decision is invalid (Oct. 6, 2015); HERMAN T. TAVANI, ETHICS AND TECHNOLOGY 167 (Beth Lang Golub ed., 4th ed. 2013); *see also* Mark Scott, *U.S.-Europe Data Transfer Agreement Is Ruled Invalid*, N.Y. TIMES, Oct. 7, 2015, at B10.

213 Communication from the Commission to the European Parliament and the Council on the Transfer of Personal Data from the EU to the United States of America under Directive 95/46/EC following the Judgment by the Court of Justice in Case C-362/14 (Schrems), COM, (2015) 566 Final (Nov. 6, 2015).

request assistance from law enforcement in foreign jurisdictions.[214] Currently, these MLATs provide procedural guidance between the United States and a foreign nation to obtain data stored abroad in order to respect that foreign nation's privacy laws.[215] The United States proffers that because warrants issued under the SCA are not effectively traditional warrants but rather are a warrant-subpoena hybrid, they do not need to go through the process the MLATs describe to request information stored in that country's data centers.[216] The rationale is the search is physically performed by the service provider, rather than a federal agent.[217] Microsoft and Ireland advocated for compliance with the guidelines set forth in the MLATs in *Microsoft II*.[218] The conflict occurs when Microsoft is directly served with the warrant, rather than the United States government adhering to the process set forth in the applicable MLAT - because while Microsoft is complying with a properly issued warrant under the SCA, it would be in violation of Ireland's laws and the Directive for turning over the user's data.[219]

The two main issues for the United States with MLATs, including MLATs with Ireland, are that the process detailed in these MLATs has been described as inefficient and laborious, and such treaties are only with approximately half of the countries in the EU.[220] The current structure of the MLATs are especially burdensome on United States law enforcement when an investigation is rapidly progressing.[221] Thus, the United States has an interest in a more expeditious process than what the MLATs currently afford.[222] In cases involving terrorism and drug trafficking, time is of the essence and compliance with an inefficient, but integral process would be a threat to the efficacy of the federal government's investigation.[223]

Compliance with warrants issued under the SCA creates a conflict between the United States and the EU because compliance with these warrants are inconsistent with the section of the Directive regarding transfer of information

---

214 Daskal, *supra* note 106, at 393.

215 *See* P. Sean Morris, *"War Crimes" Against Privacy - the Jurisdiction of Data and International Law*, 17 J. HIGH TECH. L. 1, 30 (2016) (describing the MLATs procedures generally).

216 Daskal, *supra* note 106, at 361.

217 Microsoft II, 829 F.3d 197, 214 (2d Cir. 2016).

218 *Id.* at 201.

219 Fabbrini, *supra* note 205.

220 Daskal, *supra* note 106, at 393–94.

221 30 No. 9 Int'l Enforcement L. Rep. 340.

222 Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 691 (2015).

223 *Id.*

to third parties as set forth in the currently existing MLATs.[224] The EU and more specifically, Ireland, as a Member State, have an interest in service providers operating in its country to comply with the standards set forth in the Directive and DPA to protect the personal data of its citizens, which equates to an interest in the United States' adherence to the MLATs.[225] Further, Dara Murphy, the Prime Minister of Data Protection expressed her disappointment with the United States' actions and found the extraterritorial reach "objectionable."[226] In fact, the Irish government said it would have assisted the United States with its investigation had it complied with the MLAT currently in effect between the parties.[227] Generally, MLATs include language that a party to the agreement shall obtain evidence from the other country in accordance with such other country's laws.[228] Under the MLAT between the United States and Ireland, the United States must receive approval from an Irish District Court Judge to receive information stored in a data center in Ireland.[229]

Based on the apparent distinctions in privacy laws between the EU and the United States, it is clear that a true conflict exists.[230] While the United States argues companies such as Google and Microsoft benefit from having their corporations and headquarters based in the United States, the EU retains an interest in the issues presiding over the *Microsoft II* case.[231] The data centers where Microsoft stores the information requested in the warrant and are at issue in the *Microsoft* cases are in Ireland; therefore, as a service provider, Microsoft is benefiting from the privacy laws Ireland and the EU affords its citizens.[232]

Ireland houses many data centers for United States-based companies.[233] One can infer that these companies made the conscious decision to store their data in

---

224 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 9, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); Mutual Legal Assistance in Criminal Matters, Ir.-U.S., art. III, Jan. 18, 2001, T.I.A.S. No. 13137 ("Requested Party may deny assistance if: (a) the Requested Party is of the opinion that the request, if granted, would impair its sovereignty, security, or other essential interests, or would be contrary to important public policy.").

225 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 9, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

226 Schultheis, *supra* note 222, at 680.

227 *Id.* at 680–81.

228 Russell Hsiao, *Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case*, 24 CATH. U.J.L. & TECH. 215, 240 (2015).

229 *Id.* at 240–41.

230 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 7–8, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

231 *Id.* at 8.

232 *Id.*

233 Schultheis, *supra* note 222, at 680.

Ireland and expect to benefit from the protection of the laws of Ireland.[234] For administrative convenience, it would be easier for courts in the United States to apply federal law than to apply EU law.[235] However, the courts should find a solution to appease the sovereign most impaired if its law is not applied.[236] Therefore, the courts should consider enforcing the MLAT between Ireland and the US.[237]

To strengthen international comity in the enforcement of warrants issued under Section 2703, the United States and the EU should revisit the negotiating table to procure a workable reciprocal agreement, structuring the transfer of data between the countries that would appease each country.[238] These reciprocal agreements should include language providing a mutual right on each country to provide notice to the other country if such request must be denied because it interferes with the requesting nation's privacy protections.[239] The United States and foreign governments would mutually benefit from assisting each other in investigations under these reciprocal agreements because they would provide balance between protecting the privacy of a foreign nation's citizens, and streamline procedures for obtaining information related to serious crimes and

---

234 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 7–8, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

235 *See id.* at 10 (stating that EU law is "much more severe than the U.S. standard.").

236 Under a comparative impairment approach, if an EU citizen was the user subject to the warrant issued under the SCA, the EU would be comparatively impaired because the Directive seeks to protect the privacy of its citizens. Engel v. CBS Inc., 981 F.2d 1076, 1081 (9th Cir. 1992); Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 11, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); *see* Offshore Rental Co. v. Cont'l Oil Co., 583 P.2d 721, 729 (1978) (holding that under the comparative interest approach, Louisiana's law would apply to a tort claim where the injury occurred because Louisiana had the greater interest in the case because its interest would be more impaired).

237 Brief of Amicus Curiae Jan Philipp Albrecht, Member of the European Parliament supporting Appellant at 11, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); *see, e.g.*, Dames & Moore v. Regan, 453 U.S. 654, 688 (1981) (holding that the executive branch has authority to settle claims with other countries when Congress has acquiesced to the President's acts). Here, because the power to enforce the MLAT is given to the President, the courts are not required to enforce it. *Dames & Moore*, 453 U.S. at 688.

238 Joe Uchill, *DOJ pitches agreements to solve international data warrant woes*, HILL (May 24, 2017, 5:11 PM), http://thehill.com/policy/cybersecurity/335015-doj-to-sens-bilateral-agreements-could-solve-international-data-warrant.

239 *See Hearing on Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights Before the Sen. Comm. on the Judiciary*, 115th cong. 6 (2017) (statement of Jennifer Daskal, Associate Professor, American University Washington College of Law) (describing a reciprocal notice requirement that would allow the United States and a foreign government notice of a request for data and a fair amount of time to oppose the request).

threats to national security.[240] Reciprocal agreements,[241] as compared to umbrella agreements,[242] which are similar to the current MLATs in place, would focus on cooperation between foreign governments and the United States.[243]

Under the current framework, the United States and foreign nations have to make direct requests to the government for data associated with the respective country's law enforcement investigation.[244] Therefore, if Ireland requests access to data stored in the United States, then Ireland's government must comply with the regulations of the SCA and obtain a warrant from a federal judge based on probable cause for an investigation that is local to its nation and the only connection Ireland has to the United States is that a United States-based company has information of Ireland's citizens.[245] Likewise, the United States must comply with Ireland's criminal procedure laws if it has requested its own citizen's data stored in Ireland.[246] The process for countries under the current MLAT framework is administratively inconvenient for each nation and takes an

---

240 *See id.* (describing the structure of reciprocal agreements for nations to provide notice requesting information and for the other nation as a party of the agreement to assist with disclosure or object the request).

241 *See* Jennifer Daskal & Andrew Keane Woods, *Cross-Border Data Requests: A Proposed Framework*, LAWFARE (Nov. 24, 2015, 8:00 AM), https://lawfareblog.com/cross-border-data-requests-proposed-framework (stating that reciprocal agreements in the data privacy contexts are defined as a written agreement between two countries allowing for each nation to directly request data from service providers located in another country consistent with the privacy laws of each nation).

242 *Cf.* Valsamis Mitsilegas, S*urveillance and Digital Privacy in the Transatlantic "War on Terror": The Case for a Global Privacy Regime*, 47 COLUM. HUMAN RIGHTS L. REV., Spring 2016 at 1, 65–67 (providing that the umbrella agreement currently in effect fails to cover citizens of all EU member states, which in effect would prevent citizens of those EU citizens whose country is not a party to the umbrella agreement, from seeking judicial redress for violations of their privacy rights); 5-52 DAVID BENDER, COMPUTER LAW: A GUIDE TO CYBERLAW AND DATA PRIVACY LAW § 52.05 (2017) (comparing the current umbrella agreement between the United States and the EU, which governs the transatlantic data transfers between the countries and provides a general framework for data protection, to reciprocal agreements, which are far more limited with regards to data protection that the EU wishes to achieve and is inconsistent with current EU Privacy Directive).

243 30 No. 9 Int'l Enforcement L. Rep. 340; *see* Nora Ni Loidean, *The End of Safe Harbor: Implications for EU Digital Privacy and Data Protection Law*, 19 J. INTERNET L., February 2016, at 1, 9 (describing that following Edward Snowden's leak of the National Security Agency's unauthorized surveillance of EU's computer networks, the Irish Court stated, "[the exposure revealed] gaping holes in contemporary US data protection.").

244 *See* Daskal & Woods, *supra* note 241 (describing the current process for requesting data stored in foreign nation may take upwards of 10 months).

245 *See* Alexander Dugas Battey Jr., *A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act*, 42 RUTGERS COMPUT. & TECH. L.J. 262, 270 (2016) (describing the current MLAT process where each nation may only obtain requested information for its own local investigation in accordance with the laws of the other nation).

246 *Id.*

average of ten months for the requesting party to receive its data.[247]

However, a reciprocal agreement would allow for a more streamlined process for the United States and foreign nations to receive cross-border data more efficiently and expeditiously.[248] Instead of the current time-consuming process in which government officials have to jump through hoops for evidence related to its own local investigations, each nation would be able to request the data directly from the other nation's service provider.[249] To avoid a conflict of interest and to further the interest of each nation's policies with regard to personal data, the requested party would evaluate a number of factors to determine if the incoming request is compliant with that nation's laws.[250] These factors include, but are not limited to: a showing of probable cause that a crime has occurred; whether the requesting nation has jurisdiction over the suspect; the severity of the crime; the over breadth of requested data; and the urgency of the investigation.[251] If the United States is requesting data from an EU nation, then the United States can show the user is not an EU citizen to assist the EU in protecting their citizen's fundamental rights.[252] These factors are not exhaustive, but rather allow the requested nation to determine whether it processes the data the other nation seeks using a totality of the circumstances while maintaining international comity.[253] These reciprocal agreements would foster cooperation

---

247 *See* Brief for Appellee at 52, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985) (arguing that federal law enforcement agencies prefer to issue a warrant under the SCA when permissible rather than through the MLAT process because the MLAT process does not produce immediate disclosure given the procedural and administrative conflicts of the foreign nation); *see also* Daskal & Woods, *supra* note 241.

248 Daskal & Woods, *supra* note 241.

249 *See* Matthew McKenna, *Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers*, 49 VAND. J. TRANSNAT'L L. 1417, 1444 (2016) (describing that reforming the current MLAT framework could possibly discourage countries from unilaterally obtaining data inconsistent with the laws of the foreign nation thereby alleviating the concerns expressed by Ireland that the United States ignored the MLAT in place); Daskal & Woods, *supra* note 241.

250 Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. Are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 624 (2017).

251 *Id.* at 658; Daskal & Woods, *supra* note 241. Other considerations for MLAT reform includes incorporating the privacy laws of each nation into the agreement. The United States then would incorporate the pertinent provisions of the SCA such as the definition of "content" and provide a basis for interpretation in the event there is a conflict of laws between the requesting nation and the disclosing nation. *Discussion Paper – What are the Solutions to the MLAT Problem?*, MLAT, https://www.mlat.info/policy-analysis-docs/discussion-paper-what-are-the-solutions-to-the-mlat-problem (last visited May 24, 2018).

252 Peter Swire, Justin D. Hemmings & Suzanne Vergnolle, *A Mutual Legal Assistance Case Study: The United States and France*, 34 WIS. INT'L L.J. 323, 364–55 (2016).

253 *See id.* (noting that with regards to data transfers across borders, a conflicts of law analysis requires analyzing factors, including constitutional and procedural issues to

between the United States and the EU member nations if each nation is able to expeditiously request their citizen's data in the other's territory so long as the privacy protections, as determined by the citizenship of the user, are not unjustly infringed.[254]

D. Congress and Amendments to the Stored Communications Act

1. Amending the SCA

The warrant provisions of the SCA Congress enacted in 1986 are outdated and should be revised to provide clarity to the courts and service providers.[255] Since the enactment of the SCA, technology and the use and storage of stored communication, such as emails have drastically changed. [256] The EU has also changed privacy regulations in the Directive over the past few years to maintain a high level of privacy to its citizens as technology increasingly advances.[257] The United States should follow the EU's lead given the high acclamations afforded to EU's carefully structured privacy regulations.[258] Simplifying the language and structure of the SCA given the advances in technology will afford the SCA the strength of the Fourth Amendment protection it originally sought to achieve.[259]

The distinction regarding communication stored for 180 days or more is now moot.[260] The purpose of the "180-rule" was related to property abandonment and

---

determine which nation has a greater interest in complying with requests from the other nation's law enforcement).

254 Negotiated reciprocal agreements could alleviate EU's concern that the United States could unilaterally obtain its citizens' data inconsistent with their data privacy policies. 30 No. 9 Int'l Enforcement L. Rep. 340; *see* La Marca, *supra* note 6, at 991–92 (describing how in *Microsoft II*, the United States argues that warrants issued under the SCA act more like subpoenas which calls into question whether this was the intent of Congress, because if this is deemed the correct interpretation then it would be a loophole the United States government may use to avoid the process provided for in the MLATs).

255 Press Release, D.O.J., Acting Assistant Attorney General Elana Tyrangiel Testifies before the U.S. House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations (March 19, 2013).

256 *Id.*

257 Brief for Appellant at 7–8, Microsoft II, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985).

258 *See* Swire & Kennedy-Mayo, *supra* note 250, at 628 (describing the comprehensive data privacy laws established in the EU to protect their citizen's fundamental rights).

259 *See* Allen D. Hankins, *Compelling Disclosure of Facebook Content Under the Stored Communications Act,* 17 SUFFOLK J. TRIAL & APP. ADVOC. 295, 319 (2012) (noting that revisions should be made to resolve ambiguity regarding messages using social media); Medina, *supra* note 9, at 292.

260 Press Release, D.O.J., Acting Assistant Attorney General Elana Tyrangiel Testifies before the U.S. House Judiciary Subcommittee on Crime, Terrorism, Homeland Security, and Investigations (March 19, 2013).

if an individual failed to open an email within 180-days, then the individual abandoned his or her property.[261] This provision no longer makes sense if the purpose of the SCA was to bolster privacy protections for secured communications.[262] An individual should retain their privacy over his or her emails and text messages so long as these emails are in their possession.[263] Congress should remove the 180-day language and revise the statute to encompass all electronic storage in the service provider's possession, regardless of whether the account holder has opened the email.[264] This amended language would provide clarity to the courts and protect information the SCA initially intended at its conception.[265]

Currently the SCA only provides a civil right of action for a service provider's violation of the SCA.[266] If the SCA's purpose was originally to afford stored communication Fourth Amendment protection, then the remedies should match violations of the Fourth Amendment.[267] Often the warrants issued under the SCA are pursuant to a criminal investigation.[268] If the stored communication was obtained in violation of the SCA, then the wrongful actor is not only the service provider but also law enforcement.[269] A proposed remedy for violation of the Fourth Amendment is suppression of the evidence.[270] But under the SCA, the remedy is not against the government but solely the service provider.[271] More importantly, a proper remedy would not be a civil suit, but rather the suppression of that information for the SCA to provide the Fourth Amendment protection as Congress originally intended in its enactment.[272]

2. Congress Should Pass the LEADS Act

Following the District Court's holding in the *Microsoft I*, Congress sought to

---

261 Kerr, *supra* note 21, at 1234.

262 *Id.*; Medina, *supra* note 9, at 292.

263 Kerr, *supra* note 21, at 1234.

264 In 2011, the Senate considered removing the language providing distinctions in communication held for more than 180-days by a service provider. Electronic Communications Privacy Act Amendments Act of 2011, S. 1011, 112th Cong. (2011); Medina, *supra* note 9, at 294.

265 Medina, *supra* note 9, at 292.

266 Kerr, *supra* note 21, at 1241.

267 *Id.* at 1212.

268 *Reforming the Electronic Communications Privacy Act Before the S. Comm. on the Judiciary*, 114th Cong. 2 (2015) (statement of Elana Tyrangiel, Principal Deputy Assistant Att'y Gen.).

269 Kerr, *supra* note 21, at 1242.

270 *Id.*

271 *Id.* at 1212.

272 Stephen E. Henderson, *After United States v. Jones, After the Fourth Amendment Third Party Doctrine,* 14 N. C. J. J. & TECH. 431, 437 (2013).

address the outdated language of the SCA through the Law Enforcement Access to Data Stored Abroad Act ("LEADS Act").[273] Revival of the LEADS Act would help address issues of interpretation of the Stored Communications Act.[274] The LEADS Act would resolve the two biggest issues the *Microsoft* cases presents.[275] It would provide the needed clarification regarding the definition of "warrants" under Section 2703 and limit the users to defendants subject to the jurisdiction of the United States to resolve the European Union's concerns over the access of its citizens' data to United States law enforcement.[276] EU Member states, including Ireland, have expressed their discontent with the United States' actions.[277] After the District Court's holding in the *Microsoft I* in favor of the government, Germany threatened not to use any United States-based data service provider unless the courts reversed the decision.[278]

The purpose of the LEADS Act is to alleviate the tension that arose between the United States and the EU following the District Court's decision in *Microsoft I* case by exempting non-United States citizens subjected to SCA warrants and limiting the territorial application of the SCA.[279] The LEADS Act would prohibit a warrant from requesting the information of an account holder, who is a foreign citizen.[280] The LEADS Act would limit the jurisdiction of the SCA to users who are United States citizens or subject to the jurisdiction of the applicable federal or state court.[281]

Not only will the LEADS Act address the conflict of law issues among the EU and its member nations, but it will also seek to improve the inefficiency of the MLATs which has hindered U.S. federal and state law enforcements' investigations.[282] The LEADS Act proposes to streamline the MLAT process by

---

273 Patrick Maines, *The LEADS Act and cloud computing*, HILL (Mar. 20, 2015, 7:00 AM), http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing

274 Battey, *supra* note 245, at 290–91.

275 *Id*.

276 18 U.S.C. § 2703 (2016); Battey, *supra* note 245, at 291; *see* Brian Tuinenga, *Log in to the Danger Zone: Data Privacy Under the SCA and Microsoft*, 51 VAL. U. L. REV. 291, 316 (2016) (describing the extent of warrants authorized under § 2703(a)).

277 Schultheis, *supra* note 222, at 664.

278 *Id*. at 683.

279 18 U.S.C. §§ 2701–2712 (1986); *see* Schultheis, *supra* note 222, at 683.

280 Rick Manning, *LEADS Act Stops DOJ Cloud-Based Power Grab*, HILL (Feb. 23, 2016), http://thehill.com/blogs/pundits-blog/technology/270373-leads-act-stops-doj-cloud-based-power-grab

281 S. 2871, 113th Cong. § 2(4) (2014).

282 Rebecca Eubank, *Hazy Jurisdiction: Challenges of Applying the Stored Communications Act to Information Stored in the Cloud*, 7 GEO. MASON J. INT'L COM. L. 161, 182 (2016); Viet D. Dinh & Jeffrey M. Harris, *Toward a Modern Statutory Framework for Law Enforcement Access to Electronic Communications*, BANCROFT PLLC (2015), http://www.bancroftpllc.com/wp-content/uploads/2015/07/LEADS-Act-White-Paper-for-

requiring the use of an online portal.[283] Through this online portal, other countries could submit an intake form requesting legal assistance and the federal government would prioritize other countries that utilize the portal.[284] Creating a more efficient process for requesting information and assistance in each nation's respective investigations will facilitate the United States' inclination to abide by the MLATs rather than to disrupt international comity by seeking loopholes.[285]

IV. CONCLUSION

Microsoft II is a case of first impression where the justices will seek resolve whether the warrant served on Microsoft as a service provider is permissible under the SCA. Ruling in favor of the United States would not hinder user privacy under the Fourth Amendment.[286] Further, holding in favor of the Government would not be an impermissible extraterritorial application of the SCA given the current precedent established in *Morrison*.[287] However, the Supreme Court will not be able to resolve the ambiguities in the language of the SCA nor will it effectively resolve the potential detrimental effects on comity given the interest of affected nations such as Ireland.[288] To resolve these potential issues, Congress should limit the territorial reach of the SCA, negotiate new reciprocal agreements with the EU, and fix the ambiguities and complex language in the SCA to bring it up to date with the current cross-border nature of data.[289]

---

publication.pdf.

283 Greg Nojeim, *LEADS Act Extends Important Privacy Protections, Raises Concerns*, CTR. FOR DEMOCRACY & TECH. (Sept. 18, 2014), https:// cdt.org/blog/leads-act-extends-important-privacy-protections-raises-concerns/.

284 *Id*.

285 Schultheis, *supra* note 222, at 690.

286 U.S. CONST. amend. IV; *see also* Matthew J. Hodge, *The Fourth Amendment and Privacy Issues on the "New" Internet: Facebook.com and Myspace.com*, 31 S. ILLINOIS U. L.J. 95, 100 (2006) (discussing how Facebook and Myspace comply with privacy issues that arise from law enforcement data requests).

287 Morrison v. Naat'l Austl. Bank Ltd., 561 U.S. 247, 251 (2010).

288 *Communication from the Commission to the European Parliament, The European Council, The Council, The European Economic and Social Committee and the Committee of the Regions Concerning Welcoming Foreign Direct Investment while Protecting Essential Interests*, COM (2017) 494 final (Sept. 13, 2017).

289 David Horton, *The Stored Communications Act and Digital Assets*, 67 VAND. L. REV. 1729, 1730 (2014).