Brooklyn Journal of Corporate, Financial & Commercial Law

Volume 9 | Issue 2 Article 8

2015

Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States Cloud Storage Industry

Ned Schultheis

WARRANTS IN THE CLOUDS: HOW EXTRATERRITORIAL APPLICATION OF THE STORED COMMUNICATIONS ACT THREATENS THE UNITED STATES' CLOUD STORAGE INDUSTRY

INTRODUCTION

The advancement of technology and the global shift towards cloud data storage has created major rifts throughout the legal landscape. Cloud technology has changed the way data is stored by breaking down borders and expanding jurisdictional reach. Unfortunately, congressional legislation has failed to keep pace with the rapid changes and extraterritorial nature of the tech industry.[1] The current piece of congressional legislation that oversees data privacy protection within the United States is the Stored Communications Act (SCA),[2] which was enacted as part of the broader Electronic Communications Privacy Act (ECPA) of 1986.[3] However, the SCA is now almost three decades old, and its vague application to present cloud technology and worldwide technological expansion has exposed U.S. technology companies, which utilize global cloud networks, to compliance difficulties from judicial and legislative uncertainty.[4]

A recent dispute between Microsoft and the United States Government highlighted the disparity between the globalization of data storage, international privacy rights, and current congressional legislation.[5] In what is described as a potentially "landmark case,"[6] the United States District Court of the Southern District of New York (the district court) upheld a

---

1. William Jeremy Robinson, *Free at What Cost?: Cloud Computing Privacy Under the Stored Communications Act*, 98 GEO. L.J. 1195, 1197 (2010) ("The law cannot keep up with the pace of change in computer networking. By the time legislatures or courts figure out how to deal with a new product or service, the technology has already progressed.").

2. *See* 18 U.S.C. §§ 2701–2711 (2012).

3. Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended at 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3126).

4. Orin S. Kerr, *A User's Guide to the Stored Communications Act and A Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1208 (2004). *See also* Jay P. Kesan et al., *Information Privacy and Data Control in Cloud Computing: Consumers, Privacy Preferences, and Market Efficiency*, 70 WASH. & LEE L. REV. 341, 401 (2013) ("The status of the SCA is problematic because much of the language is very unclear or outdated and interpretations of the statute by courts have varied significantly."); Illana R. Kattan, Note, *Cloudy Privacy Protections: Why the Stored Communications Act Fails to Protect the Privacy of Communications Stored in the Cloud*, 13 VAND. J. ENT. & TECH. L. 617, 645 (2011) ("Because Congress enacted the SCA as part of ECPA in the late 1980s and has not amended it to address cloud computing, the ECPA—specifically, the SCA—needs to be revisited.").

5. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) [hereinafter *In re* Warrant I Mag. J.].

6. Ellen Nakashima, *Microsoft Fights U.S. Search Warrant for Customer E-mails Held in Overseas Server*, WASH. POST (June 10, 2014), http://www.washingtonpost.com/world/national-security/microsoft-fights-us-search-warrant-for-customer-e-mails-held-in-overseas-server/2014/06/10/6b8416ae-f0a7-11e3-914c-1fbd0614e2d4_story.html.

warrant under the SCA[7] requiring Microsoft to disclose personal data, in particular private e-mails of a Microsoft e-mail user, stored on Microsoft servers in Dublin, Ireland.[8] The search warrant relates to an ongoing narcotics investigation in the United States.[9] The warrant was originally issued by a magistrate judge, who "held that [the] warrant did not violate [the] presumption against extraterritorial application of the law of the United States,"[10] and was affirmed by a U.S. District Court Judge on appeal.[11]

In response to the issuance of the warrant, major U.S.-based tech companies have been in a frenzy to appeal the decision and argue for new or amended federal legislation to help prevent potential backlash from the international community.[12] Microsoft and other technology and telecommunications giants, including Verizon Communications Inc.; AT&T, Inc.; Apple Inc.; Cisco Systems, Inc.; among others (collectively, U.S. Technology Companies),[13] are afraid that the expansion of a search warrant's extraterritorial reach, especially to non-U.S. citizens, would cause "foreign individuals and businesses [to] flee to their non-U.S. competitors."[14] Verizon, AT&T, Apple, Cisco Systems, and the privacy group, Electronic Frontier Foundation, have filed amicus briefs in support of Microsoft's opposition to the extraterritorial reach of the warrant.[15] These technology giants are dedicated to global data storage and transfer, serving clients from around the world.[16] Most importantly, these companies, in particular Microsoft, sell cloud storage to multi-national corporations who pay Microsoft to keep personal information and communication secured on their servers. However, after the district court's decision to uphold the warrant, the expanding reach of a vague and dated statute further restrains

---

7. *See* 18 U.S.C. §§ 2703(a)–(d).

8. *In re* Warrant I Mag. J., *supra* note 5, at 467.

9. *Id.*

10. *Id.* at 466.

11. *See* Transcript of Oral Argument at 69, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) [hereinafter Transcript of July 31 Order]. *See also In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) [hereinafter *In re* Warrant II C.J.] (granting a motion to lift the stay of the Court's July 31, 2014 order "affirming the April 25, 2014 decision of Magistrate Judge James C. Francis IV").

12. Larry Neumeister, *The US Government Can Force Microsoft to Turn Over Emails, Even If They're Stored Overseas*, BUS. INSIDER (July 31, 2014), http://www.businessinsider.com/judge-rules-against-microsoft-us-warrants-ireland-2014-7.

13. *See* Motley Fool, *Microsoft, Apple, and Amazon Unite Against a Common Foe*, NASDAQ (Dec. 17, 2014, 4:31:02 PM), http://www.nasdaq.com/article/microsoft-apple-and-amazon-unite-against-a-common-foe-cm424469.

14. Nakashima, *supra* note 6.

15. Allison Grande, *Microsoft Must Cough Up Data Stored Overseas*, *Judge Rules*, LAW360 (July 31, 2014), http://www.law360.com/articles/562289/microsoft-must-cough-up-data-stored-overseas-judge-rules.

16. *See* Motley Fool, *supra* note 13.

Microsoft and other U.S.-Technology Companies that rely on cloud data networks.[17]

Microsoft, Verizon, and Cisco are all still reeling from international damage caused by Edward Snowden's mass leak of U.S. National Security Agency (NSA) surveillance programs,[18] which exposed the U.S. government's widespread infringement of both U.S. and foreign citizens' privacy through phone wiretaps and internet surveillance.[19] The district courts' recent affirmation of the SCA warrant against Microsoft, in allowing the U.S. government to seize private electronic communication stored abroad without going through the traditional bilateral channels[20] to obtain such evidence, further heightens fears of U.S. privacy intrusion both at home and aboard. This places a strong burden on U.S. Technology Companies to interpret unclear and dated congressional legislation and attempt to construct a coherent and precise compliance policy for their business to assure certain privacy protections to their customers without violating domestic or international law.[21] Without a clear compliance policy outlining specific privacy protections for customers' data stored around the world on global networks, Microsoft and other U.S. cloud companies risk losing large sums of business to either foreign data storage companies or data localization movements in the hopes of sheltering customers from the expansive jurisdictional reach of the SCA warrant.[22]

Ultimately, the unclear application of the dated and vague SCA leads to impractical compliance problems for U.S. Technology Companies, thereby threatening their economic growth. As long as U.S. legislation lags behind, U.S. Technology Companies are at risk to losing business with international

---

17. *Id.*

18. Nakashima, *supra* note 6.

19. The extent of the NSA's surveillance was profoundly troubling due to the discovery that the NSA specifically targeted foreign officials, particularly in the E.U, for surveillance. *See* Josh Levs & Catherine E. Shoichet, *Europe Furious, 'Shocked' by Report of U.S. Spying*, CNN (Jul. 1, 2013, 7:14 AM), http://www.cnn.com/2013/06/30/world/europe/eu-nsa/.

20. The traditional bilateral process for requests for evidence located outside the United States is through Mutual Legal Assistant Treaties (MLAT), which the United States has with Ireland. *See* Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, U.S.-Ire., Jan. 18, 2001, T.I.A.S. 13137 [hereinafter U.S.-Ire. MLAT].

21. *See generally* Jan. P. Levine, *Feds Pose Privacy Risk By Grabbing Overseas ISP Emails*, LAW360 (Sept. 8, 2014, 10:27 AM), http://www.law360.com/articles/574533/feds-pose-privacy-risk-by-grabbing-overseas-isp-emails ("Left unchanged, Judge Preska's ruling creates significant risks for any company subject to U.S. jurisdiction by weakening its ability to protect its customers' information, abolishing distinctions between a company's own business records and its customers' private correspondence, and subjecting companies to potential sanctions for violating privacy laws of the countries in which they locate their data centers.").

22. *See generally* Steve Pociask, *Spy in the Clouds: How DOJ Actions Could Harm U.S. Competitiveness Abroad*, AM. CONSUMER INST. CTR. FOR CITIZEN RESEARCH (2014), http://www.theamericanconsumer.org/wp-content/uploads/2014/09/Balkanized-Internet.pdf (arguing that the Department of Justice's legal overreach to seize e-mails located in Ireland by use of warrant will have negative economic implications for U.S. cloud companies operating abroad).

customers and nations, potentially amounting to lost profits in the billions of dollars.[23] In addition, the extraterritorial application of the SCA places pressure on international relations, particularly between the United States and the European Union (the E.U.), over data protection law,[24] which only further constrains the U.S. technology and cloud data industry. Microsoft's ongoing legal battle with the U.S. government[25] highlights what is likely to be a recurrent debate over the expanding jurisdictional reach of the United States with electronic information now commonly stored abroad. Instead of forcing the courts to interpret congressional legislation, this issue demands legislators to re-think lagging statutes that relate to electronic information and to take a more pro-active approach so that legislation more accurately reflects advances in technology. This Note recommends certain amendments to the SCA to improve its relevancy to modern technology, based on the newly introduced Senate bill entitled the Law Enforcement Access to Data Stored Abroad Act (the LEADS Act).[26]

Part I of this Article looks generally at the legislative history behind the formation of the ECPA and SCA statutes alongside the evolution of the Internet from both a technological and legislative standpoint. Part II analyzes Magistrate Judge Francis's order granting the SCA warrant to obtain private emails located on Microsoft servers in Dublin, Ireland. Part III looks at the district court's decision to uphold the SCA warrant against Microsoft. Part IV looks at the compliance consequences this ruling has on U.S. Technology Companies, and various aspects the district court's ruling has on both Microsoft's compliance with international law, particularly in the E.U. Additionally, it discusses Microsoft's ability (or in-ability) to create sufficient privacy protections to match customer expectations. Part V looks specifically at the economic consequences these compliance problems have on U.S. Technology Companies from a business perspective. Finally, Part VI looks at the newly introduced bill in the House and Senate entitled the LEADS Act,[27] which has been introduced in direct response to the

23. *See id.* at 2.

24. John O'Connor, *The Microsoft Warrant Case: Not Just an Irish Issue*, LEXOLOGY (Oct. 8, 2014), http://www.lexology.com/library/detail.aspx?g=2b7ab8cb-f618-47b5-b56f-310b0112772a (explaining the continued discomfort in the E.U., in particular Germany, with the United States' stance on data privacy and the global ramifications of the District Court's decision to uphold the SCA warrant).

25. *See generally In re* Warrant I Mag. J., *supra* note 5; Transcript of July 31 Order, *supra* note 11; *In re* Warrant II C.J., *supra* note 11.

26. "To amend title 18, United States Code, to safeguard data stored abroad from improper government access, and for other purposes." The Law Enforcement Access to Data Stored Abroad Act, S. 2871, 113th Cong. (2014) [hereinafter The LEADS Act].

27. This bill is brought by Senators Orrin Hatch (R-UT), Chris Coons (D-DE), and Dean Heller (R-NV) "[t]o amend title 18, United States Code, to safeguard data stored abroad from improper government access, and for other purposes." *Id.*

district court's approval of the SCA warrant,[28] and suggests that further refinement of the SCA can promote a more efficient legal procedure for allowing the U.S. government to obtain electronic evidence related to a criminal proceeding located outside the United States.

I. LEGISLATIVE HISTORY OF ECPA AND SCA

The U.S. government's alleged power to issue the conflicted warrant comes from the SCA[29] as part of the ECPA.[30] In order to understand the SCA warrant, we must examine the formation of the ECPA and SCA statutes themselves and consider their relation to traditional federal criminal procedures and the rise of the Internet in the 1980s.

During the mid-1980's, Congress had become aware that the various advancements in technology, including the wireless telephone, home computer, and internet, were leaving holes in "existing privacy protections for communications and stored electronic records."[31] Although relatively few Americans had home computers or used the internet in 1986, businesses from the mid-1980's onward began using electronic communication with increasing frequency.[32] In the past, corporate users connected to a private network via modem to communicate with one another. Corporate employees would utilize their company's private server to send e-mails, post messages on shared "bulletin boards," or access company stored information.[33] This growing change in communications concerned policy-makers and civil liberties organizations seeking to remedy the situation through legislation aimed to protect privacy in electronic communications.[34] As a result, Congress enacted the ECPA in 1986 to encompass a broad range of telecommunications and electronic communications privacy rights.[35]

Structurally, the ECPA was separated into three distinct titles or acts: the Wiretap Act,[36] the Pen Register statute,[37] and most importantly for the

28. *See In re* Warrant I Mag. J., *supra* note 5, at 477; Transcript of July 31 Order, *supra* note 11; *In re* Warrant II C.J.*, supra* note 11.

29. *See* 18 U.S.C. §§ 2701–2711 (2012).

30. *See* 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3126.

31. Deirdre K. Mulligan, *Reasonable Expectations in Electronic Communications: A Critical Perspective on the Electronic Communications Privacy Act*, 72 GEO. WASH. L. REV. 1557, 1559 (2004).

32. *Id.* (noting that much of the expansion in the mid-1980s of businesses' use of e-mail was from a leveraged move by AT&T to enter the electronic mail market, which was expected to grow exponentially over a few years) (citing Melissa Calvo & Jim Forbes, *AT&T's E-Mail Enters Slow Market*, INFOWORLD, Mar. 10, 1986, at 5).

33. Robinson, *supra* note 1, at 1198.

34. Mulligan, *supra* note 31, at 1561.

35. *See* 18 U.S.C. §§ 2510–2522, 2701–2712, 3121–3126.

36. *See id.* §§ 2511–2522.

37. *See id.* §§ 3121–3127.

purpose of this note, the SCA.[38] The SCA originated to alleviate Fourth Amendment concerns arising from the creation of the Internet.[39] The Internet's expansion into everyday life left a legislative void for the constitutional protection over searches and seizures of "virtual homes" created in cyberspace.[40] The Fourth Amendment gives privacy protection to "homes in the physical world"; however, "virtual homes" of the Internet were left unguarded to government intrusion and privacy violation.[41] In criminal procedure under the protection of the Fourth Amendment, "absent special circumstances, the government must first obtain a search warrant based on probable cause before searching a home for evidence of crime."[42] The SCA attempted to provide the necessary privacy protection of information stored on the Internet.[43] As the Internet came to dominate our everyday lives, "our most private information ends up being sent to private third parties and held far away on remote network servers."[44]

When the ECPA was first enacted in 1986, it was hailed "as a victory for privacy,"[45] despite that personal computers were a rarity and the Internet was predominately used only commercially.[46] Still, even in the mid-1980's, there was a growing consensus in Congress that existing privacy laws were incapable of handling the budding technological advances of the time.[47] Although once considered a landmark piece of legislation, today there is a consensus among members of Congress,[48] technology giants,[49] and industry

38. *See id.* §§ 2701–2711; Mulligan, *supra* note 31, at 1565.

39. Kerr, *supra* note 4, at 1210.

40. *Id.*

41. *Id.* at 1209.

42. *Id.* ("At the very core of the Fourth Amendment stands the right of a man to retreat into his own home and there be free from unreasonable governmental intrusion. With few exceptions, the question whether a warrantless search of a home is reasonable and hence constitutional must be answered no." *Id.* at 1209 n.8 (quoting Kyllo v. United States, 533 U.S. 27, 31 (2001))).

43. *Id.* at 1210.

44. *Id.* at 1209–10. This expansion of personal data stored globally by third parties creates incredible strains on the ability of the Fourth Amendment to protect our personal information. *Id.* at 1210 ("This feature of the Internet's network architecture has profound consequences for how the Fourth Amendment protects Internet communications—or perhaps more accurately, how the Fourth Amendment may not protect such communications at all.").

45. Mulligan, *supra* note 31, at 1557 (citing 132 CONG. REC. H4045-46 (daily ed. June 23, 1986) (statement of Rep. Kasternmeier) (noting that "broad bipartisan support" in conjunction with a "coalition of business, Government and civil liberties groups" brought the bill to fruition)).

46. *Id.* ("In 1986, relatively few people had Internet access; commercial electronic mail services and commercial data processing center were emerging, but both primarily served the business community.").

47. *Id.* at 1559 (according to Professor Mulligan, "members of Congress, the telecommunications and computing industry, and civil libertarians," were aware "that advances in telecommunications, such as wireless telephones and e-mail, were outpacing existing privacy protections for communications and stored electronic records").

48. Senators Orrin Hatch (R-UT), Chris Coons (D-DE), and Dean Heller (R-NV) recently reintroduced the LEADS Act to the Senate floor. *See Senator Coons Reintroduces Bill to Protect Americans' Electronic Data Stored Abroad*, U.S. SEN. CHRISTOPHER COONS OF DE. (Feb. 12, 2015), http://www.coons.senate.gov/newsroom/releases/release/senator-coons-reintroduces-bill-

professionals that the legislation is now dated in comparison to the far-reaching advancements in technology.[50]

The SCA is no longer relevant given the exponential increase of Internet usage in the United States in recent years. The SCA originated from a time far different from today's global network.[51] It is now almost impossible to go through life without constantly interacting with the Internet. Even in 2004, before cloud technology further expanded the ability of companies to store electronic information, there was already "an enormous growth in personal use of the Internet."[52] Most recently, in 2014, statistical evidence shows roughly 87% of Americans used the Internet in comparison to the 66% of Americans that used the Internet in 2005.[53] The results are even more dramatic when compared to the only 14% of Americans that used the Internet as recent as 1995.[54] The Internet is only going to continue to grow as a prominent part of everyday life for Americans and people around the world.

---

to-protect-americans-electronic-data-stored-abroad. Additionally, Representatives Tom Marino (R-PA) and Suzan DelBene (D-WA) recently introduced the LEADS Act to the House of Representatives. *See* Emily Field, *House Reps. Propose Bill On Overseas Data Storage*, LAW360 (Feb. 27, 2015, 5:03 PM), http://www.law360.com/articles/626089/house-reps-propose-bill-on-overseas-data-storage.

49. *See* Andrew Keshner, *Microsoft Loses Bid to Quash U.S. Warrant*, N.Y. L.J. (Aug. 1, 2014), http://www.newyorklawjournal.com/id=1202665397289/Microsoft-Loses-Bid-to-Quash-US-Warrant?slreturn=20141120170027 ("Technology giants like Apple, Cisco Systems, Verizon and AT&T filed amicus briefs supporting Microsoft."). *See also* Chris Versace, *Opinion: LEADS Act Can Save U.S. Innovation*, FOX BUS. (Feb. 23, 2015), http://www.foxbusiness.com/technology/2015/02/23/opinion-leads-act-can-save-us-innovation/ ("The response from technology companies and associations such as Apple (AAPL), IBM (IBM), Cisco Systems, Internet Infrastructure Coalition (i2 Coalition) . . . has been one of positive support for the LEADS Act.").

50. Mulligan, *supra* note 31, at 1559 ("The changed ways in which people use the Internet, enabled by new technical standards, laws, and business models, have exposed fundamental weaknesses in the structure of the ECPA. Many who supported the statute would agree that it has failed to keep pace with changes in and on the Internet and therefore no longer provides appropriate privacy protections. It is time to revisit and revise ECPA to establish appropriate privacy protections that respect individuals' expectations and constitutional requirements."). This statement from Professor Mulligan is even more telling today, because within the past decade cloud technology has further expanded the gap between the ECPA's relevance and the technology it presumably protects.

51. *See generally* Robinson, *supra* note 1, at 1196–97 ("The Stored Communications Act (SCA) . . . is the primary federal source of online privacy protections, but it is more than twenty years old. Despite the rapid evolution of computer and networking technology since the SCA's adoption, its language has remained surprisingly static. The resulting task of adapting the Act's language to modern technology has fallen largely upon the courts.").

52. Mulligan, *supra* note 31, at 1557–58 (describing how millions of individuals use the Internet in a multitude of ways as part of everyday life, including e-mails, online chats, photo albums, journals, blogs, etc., and how that information is stored on commercial servers).

53. *See* SUSANNAH FOX & LEE RAINIE, PEW RESEARCH CTR., THE WEB AT 25 IN THE U.S. 17 (2014), *available at* http://www.pewInternet.org/files/2014/02/PIP_25th-anniversary-of-the-Web_0227141.pdf.

54. *Id.*

II. MAGISTRATE JUDGE'S SCA WARRANT APPROVAL FOR EXTRATERRITORIAL APPLICATION

> The 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.[55]

This ominous and foretelling depiction of the divergence between law and technology is the specially chosen opening remarks of Magistrate Judge James C. Francis IV, who was presented with the task of applying old legislation to modern technology.[56] On December 4, 2013, U.S. government authorities, in connection with an ongoing narcotics investigation within the United States, secured a search warrant from Magistrate Judge Francis pursuant to the SCA[57] for the contents of a Microsoft customer's private e-mail account.[58] Specifically, the SCA warrant required Microsoft to disclose:

a) the contents of all e-mails stored in the specified user's account, including those sent;
b) all records or other information regarding the identification of the user of the account (such as name, address, phone number etc.);
c) all records or information stored on account including address books, contact lists, pictures, and files; and finally
d) all records of communication between the user and Microsoft Network (MSN).[59]

Once Microsoft realized that the user data associated with the requested Microsoft account was not stored on servers domestically within the United States but on servers located in Ireland, Microsoft filed a motion to quash the warrant.[60] Essentially, Microsoft challenged the extraterritorial application of the SCA warrant. Microsoft stated it was not within the U.S. government's authority to issue the search and seizure of information or documents from a foreign country without going through the proper criminal procedural channels in place for retrieving documents located abroad.[61]

---

55. *In re* Warrant I Mag. J., *supra* note 5, at 467 (citing David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1375 (1996)).

56. *Id.*

57. 18 U.S.C. §§ 2703(a)–(d) (2012).

58. Joseph Falcone, *US Federal Court Orders Microsoft to Produce E-mail Contents Stored Outside the United States*, HERBERT SMITH FREEHILLS DISP. RESOL. (Aug. 5, 2014), http://www.herbertsmithfreehills.com/-/media/Files/ebulletins/2014/20140805%20-%20ny%20e-bulletin%20microsoft%20decision.html; *In re* Warrant I Mag. J., *supra* note 5, at 467–68.

59. *In re* Warrant I Mag. J., *supra* note 5, at 468.

60. *Id.*

61. This is referencing the MLAT, which is an agreement between nations (such as the one in existence between the United States and the Republic of Ireland) in which the countries agree to assist one another in criminal investigations, including the retrieval of documents for evidentiary

The court ultimately denied Microsoft's motion to vacate and upheld the issuance of the warrant.[62] The court was more concerned with the process of *how* the SCA warrant worked in obtaining electronic information than with the actual location of the information. As the court explains, the SCA warrant is "hybrid: part search warrant and part subpoena."[63] In order to first obtain the warrant order, "the Government must provide the court with 'specific and articulable facts showing that there are reasonable grounds to believe that the content of a wire or electronic communication, or the records or other information sought, are relevant and material to an ongoing criminal investigation.'"[64] In other words, to obtain the SCA warrant, the Government must follow traditional criminal warrant procedures described in the Federal Rules of Criminal Procedure and demonstrate probable cause to a magistrate judge.[65] Once the Government has made a sufficient showing of probable cause or reasonable suspicion to a neutral magistrate judge, the Government can "compel a service provider to disclose everything that would be produced in response to a section 2703(d) order or a subpoena as well as unopened e-mails stored by the provider for less than 180 days."[66]

However, what makes the SCA warrant a "hybrid order" is that unlike a traditional warrant which requires U.S. government agents to physically enter the premises and seize the authorized documents,[67] the SCA order is "executed like a subpoena in that it is served on the ISP [Internet Service Provider] in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the e-mail account in question."[68] The nature of the warrant applying to electronic data information allows the performance of the warrant and the seizure of the data to be completed at any remote location from a certified computer. Therefore, U.S. government agents would not have to travel to Ireland and infiltrate the Microsoft server base to seize the e-mails associated with the

---

purposes. *See* U.S.-Ire. MLAT, *supra* note 20. The current MLAT procedure, however, as argued by the United States and stated by Magistrate Judge Francis, is "slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other." *In re* Warrant I Mag. J., *supra* note 5, at 474 (citing Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PENN. L. REV. 373, 409 (2014)).

62. *In re* Warrant I Mag. J., *supra* note 5, at 477.

63. *Id.* at 471.

64. *Id.* at 469 (citing 18 U.S.C. § 2703(d)).

65. *Id.* at 470 (citing 18 U.S.C. § 2703(a)). *See also* FED. R. CRIM. P. 41(d)(1) (requiring probable cause for warrants).

66. *In re* Warrant I Mag. J., *supra* note 5, at 470. In particular, an order under § 2703(d) entitles the Government to "all information subject to production under a subpoena and also 'record[s] or other information pertaining to a subscriber [] or customer,' such as historical logs showing the e-mail addresses with which the customer had communicated." *Id.* at 469 (citing 18 U.S.C. § 2703(c)(1)).

67. *See* FED. R. CRIM. P. 41 (statute for traditional criminal warrant procedures in the United States).

68. *In re* Warrant I Mag. J., *supra* note 5, at 471.

suspected user. Instead, they could use any Microsoft computer within the United States, so long as the computer has the proper user information and e-mail retrieval software to view the pertinent stored information.[69] According to the court, "this unique structure supports the Government's view that the SCA does not implicate principles of extraterritoriality."[70]

In continuance with the notion that SCA § 2703 is a "hybrid warrant," the court shifted its focus from the requirement to show "probable cause" akin to warrant procedures[71] to the principles and procedures for obtaining a subpoena, which requires the production of information within a party's "possession, custody, or control regardless of the location of that information."[72] The appropriate test for document production, according to the court, therefore, is not one of location, but is instead one of *control*.[73] The court found that it did not matter where the data for the e-mails was located so long as Microsoft had control or possession over them.[74] Moreover, the court found in terms of a "search and seizure" in the digital age, the search occurs when a person views the information on a computer screen (such as viewing the e-mail as you normally would on a computer), rather than the search occurring at the server location (i.e., the physical location of the server).[75]

Another prominent issue of contention was whether Congress intended for the SCA warrant to reach or apply extraterritorially.[76] When Congress

---

69. *Id.* at 468 (stating that Microsoft's Global Criminal Compliance (GCC) team members can use "a database program or 'tool' to collect the data" stored in Dublin, Ireland by initially using the "tool" to locate where the target account is stored and then to collect the information or data associated with that account remotely from the server, wherever it is located).

70. *Id.* at 472.

71. *See* FED. R. CRIM. P. 41.

72. *In re* Warrant I Mag. J., *supra* note 5, at 472.

73. *Id.* ("Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location." (quoting Matter of Marc Rich & Co., A.G., 707 F.2d 663, 667 (2d Cir. 1983))).

74. Magistrate Judge Francis does not go into much depth detailing the court's definition of "control" in this opinion. Instead, as explained later in this Note, Chief Judge Preska explores in more detail Microsoft's "control" in this instance, associating it with the *Bank of Nova Scotia* doctrine. *See* Levine, *supra* note 21; Transcript of July 31 Order, *supra* note 11.

75. "[A] search occurs when information from or about the data is exposed to possible human observation, such as when it appears on a screen, rather than when it is copied by the hard drive or processed by the computer." *In re* Warrant I Mag. J., *supra* note 5, at 472 (quoting Orin S. Kerr, *Searches and Seizures in a Digital World*, 119 HAR. L. REV. 531, 551 (2005)).

76. *Id.* at 470–74. The court goes on to quote the Senate:

> The Committee also recognizes that computers are used extensively today for the processing and storage of information. With the advent of computerized recordkeeping systems, Americans have lost the ability to lock away a great deal of personal and business information. For example, physicians and hospitals maintain medical files in offsite data banks, business of all sizes transmit their records to remote computers to obtain sophisticated data processing services . . . . [B]ecause it is subject to control by a third party computer operator, the information may be subject to no constitutional privacy protection.

enacted the SCA as part of the ECPA, it did not expressly cover the issue of its extraterritorial application.[77] However, even though the Senate report "did not address the specific issue of extraterritoriality," the court felt there "reflected an understanding that information was being maintained remotely by third-party entities."[78] Microsoft argued that the U.S. Supreme Court previously held that a presumption against extraterritoriality exists when Congress has not given "clear indication of an extraterritorial application" within the language of the statute or explicitly noted otherwise.[79] However, the court rejected Microsoft's argument. The court stated that the existence of "the nationality principle," which recognizes that American criminal laws can apply outside the United States to legal entities subject to the jurisdiction of the United States, may require U.S. companies, such as Microsoft, to obtain evidence located aboard in connection with an ongoing domestic criminal investigation.[80]

To help its argument on the ambiguity of Congress's extraterritorial intent for the SCA, the court used other pieces of Congressional legislation to fill in the holes left by Congress within the SCA statute itself.[81] The court looked to the legislative history of the Uniting and Strengthening America By Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (the Patriot Act) for guidance and found that Section 108 of the Patriot Act allows "nationwide service of search warrants for electronic evidence."[82] Specifically, the House Committee stated the incredible time sensitivity of suspected terrorist's criminal proceedings

---

Id. at 472–73 (citing S. REP. NO. 99-541, at 3 (1986)).

77. *Id.* at 472.

78. *Id.*

79. *Id.* at 475 ("The presumption against territorial application provides that 'when a statute gives no clear indication of an extraterritorial application, it has none,' *Morrison v. National Australian Bank Ltd.*, 561 U.S. 247, 255, 130 S.Ct. 2869, 2878, 177 L.Ed.2d 535 (2010), and reflect the 'presumption that United States law governs domestically but does not rule the world,' *Microsoft Corp. v. AT&T Corp.,* 550 U.S. 437, 454, 127 S.Ct. 1746, 167 L.Ed.2d 737 (2007).").

80. *Id.* at 476. The court rationalizes this statement by claiming that the SCA warrant does not criminalize any conduct outside the United States and does not initiate the deployment of United States law enforcement agents abroad, but instead only extends "American criminal law outside the nation's borders." *Id.* The court quotes *Blackmer v. United States*, 284 U.S. 421 (1932) (requiring the return of a sanctioned witness after their refusal to return from abroad to testify in a US criminal proceeding) in support of the 'nationality principle,' stating:

> With respect to such an exercise of authority, there is no question of international law, but solely of the purport of the municipal law which establishes the duty of the citizen in relation to his own government. While the legislation of the Congress, unless the contrary intent appears, is construed to apply only within he territorial jurisdiction of the United States, the question of its application, so far as citizens of the United States are concerned, is one of construction, not of legislative power.

Id.

81. *In re* Warrant I Mag. J., *supra* note 5, at 472–74.

82. This "nationwide service of search warrants" is different from the traditional approach contained in FED. R. CRIM. P. 41, which requires the warrant to be obtained "within the district" where the property is located. *Id.* at 473.

rationalized the expansion of national search warrants.[83] The House Committee was focused on the potentially devastating "investigative delays caused by the cross-jurisdictional nature of the Internet."[84] The Patriot Act allows a warrant under § 2703 to reach throughout the United States, so long as the ISP was located within the United States.[85] Therefore, it does not matter where the actual server that stored the electronic information (e-mails, etc.) was located.[86] The court interpreted the focus on the location of the ISP as opposed to the location of the actual server as evidence that Congress had "anticipated that an ISP located in the United States would be obligated to respond to a warrant issued pursuant to section 2703(a) by producing information within its control, regardless of where that information was stored."[87] Based on the courts' interpretation of congressional legislative history, the court ultimately upheld the SCA warrant forcing Microsoft to disclose the e-mails located in Dublin, Ireland.

III. U.S. DISTRICT COURT UPHOLDS MAGISTRATE JUDGE'S EXTRATERRITORIAL WARRANT

After Microsoft appealed to Federal Court, Chief U.S. District Court Judge Loretta A. Preska in a July 31, 2014 hearing, ruled from the bench and dismissed Microsoft's motion to quash the SCA warrant, upholding the Magistrate Judge's warrant.[88] The district court decided that the dispute came down to a "question of control, not a question of location."[89] So long as Microsoft had control over the user's e-mails and was able to access them within the United States, the court found no reason why Microsoft should be precluded from disclosing the e-mails in connection with a domestic criminal investigation. The fact that the e-mails' data happened to be stored abroad on servers located in Ireland did not diminish Microsoft's

---

83. *Id.* (citing H.R. REP. 107-236(I), at 58 (2001)).
84. *Id.*
85. *Id.*
86. *Id.*at 473–74 (citing H.R. REP. 107-236(I), at 58 (2001)).
87. *Id.* at 474.
88. Keshner, *supra* note 49.
89. Transcript of July 31 Order, *supra* note 11, at 69. Chief Judge Preska refers to Magistrate Judge Francis's statement:

> [I]t has long been the law that subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information. *See Matter of Marc Rich & Co., A.G.,* 707 F.2d 663, 667 (2d Cir.1983) ('Neither may the witness resist the production of documents on the ground that the documents are located abroad. The test for production of documents is control, not location.' (citations omitted)); *Tiffany (NJ) LLC v. Qi Andrew,* 276 F.R.D. 143, 147–48 (S.D.N.Y. 2011) ('If the party subpoenaed has the practical ability to obtain the documents, the actual physical location of the documents—even if overseas—is immaterial.'); *In re NTL, Inc. Securities Litigation,* 244 F.R.D. 179, 195 (S.D.N.Y. 2007); *United Sates v. Chase Manhattan Bank, N.A.,* 584 F.Supp. 1080, 1085 (S.D.N.Y.1984).

In re Warrant I Mag. J., *supra* note 5, at 472.

control nor inhibit domestic access to the electronic information.[90]To better understand the economic and policy consequences the district court's decision has on U.S. Technology Companies, Part III of this Note takes an in-depth look at the various arguments between the U.S. Government and Microsoft, resulting in the court's decision to uphold the SCA warrant.

A. THE *BANK OF NOVA SCOTIA* DOCTRINE AND ISSUE OF "CONTROL"

The district court used a 1984 U.S. Court of Appeals for the Eleventh Circuit case, *In re Grand Jury Proceedings* (*Bank of Nova Scotia*), to support its decision to uphold the SCA warrant.[91] The *Bank of Nova Scotia* case "permitted the disclosure of records stored in the Bahamas and maintained by a Canadian bank with U.S. branches,"[92] and is known as "the Bank of Nova Scotia Doctrine" (the BNS doctrine).[93] Under the BNS doctrine, "a grand jury subpoena can be used to compel a company subject to U.S. jurisdiction to produce evidence stored outside the United States if the evidence is within the company's possession, custody, or control."[94] Although the documents ordered for disclosure in *Bank of Nova Scotia* were banking records of U.S. citizens as opposed to third-party private e-mails of a citizen whose country of origin has not yet been disclosed,[95] the court held that the BNS doctrine still applied to Microsoft in this case to force disclosure.[96]

Microsoft argued that this discrepancy in the types of documents forced to be disclosed made the present Microsoft motion distinct from the *Bank of Nova Scotia* case and doctrine.[97] Microsoft argued there was "'a world of difference,' between a bank being compelled to turn over its own records and Microsoft's being compelled to produce a customer's e-mail

90. Keshner, *supra* note 49.

91. *In re* Grand Jury Proceedings (Bank of Nova Scotia), 740 F.2d 817 (11th Cir. 1984).

92. Keshner, *supra* note 49.

93. Levine, *supra* note 21.

94. *Id.*

95. The BNS court applied a "balancing interests" test to compare the interests of the U.S. government to pursue their criminal investigation and the interests of American citizens to have their bank records remain private. The court found that the interests of the U.S. government in pursuing a criminal investigation outweighed those of an individual's right to privacy. *Bank of Nova Scotia,* 740 F.2d at 828 ("The interest of American citizens in the privacy of their bank records is substantially reduced when balanced against the interests of their own government engaged in a criminal investigation since they are required to report those transactions to the United States pursuant to 31 U.S.C. § 1121 and 31 C.F.R. § 103.24 (1979). *United States v. Payner,* 447 U.S. 727, 732 and n. 4, 100S.Ct. 2439, 2444 and n. 4, 65 L.Ed. 2d 468 (1980).").

96. It could be argued that the requirement for the Bank of Nova Scotia to report the relevant bank transactions to the U.S. government is distinguishable from the private emails of third party customers to Microsoft, who have no such requirement to report.

97. Keshner, *supra* note 49. *See also* Falcone, *supra* note 58 ("[P]er Microsoft, the actual content of these e-mails were not company records, but were private information of its customer and thus entitled to heightened constitutional protection.").

correspondence."[98] They claimed these private and personal e-mails stored on Microsoft servers limited the BNS doctrine's application because the documents were contained in a "digital lockbox," where customers had a certain expectation of privacy.[99] Microsoft said that these private conversations were distinguishable from the transactional banking records of the *Bank of Nova Scotia* and therefore, were not under the same "control" standard as established under the BNS doctrine.[100]

The U.S. government countered by dismissing Microsoft's asserted limitations to the BNS doctrine. They reiterated that "control" was all that mattered. According to the U.S. government, the BNS doctrine of "control" was satisfied because Microsoft could transfer, view, and supply the contentious e-mails to the U.S. government.[101] In the end, the court concluded that Microsoft had waived its right to argue that the documents were not their own business records, but rather the documents of its customers in order to distinguish this case from the BNS doctrine.[102] With the arguments waived, the court found the private e-mails were under Microsoft's "control" and therefore followed the Magistrate Judge's conclusion that it was a matter of control, not location in demanding disclosure under the SCA.[103]

B. CONGRESSIONAL INTERPRETATION OF BNS AND EXTRATERRITORIAL APPLICATION OF SCA

In determining whether Congress intended for the SCA to apply extraterritorially, the court found there was sufficient evidence to infer that

98. Keshner, *supra* note 49.

99. Levine, *supra* note 21.

100. *Id.*

101. Serrin Andrew Turner, the Assistant U.S. Attorney for the S.D.N.Y. who represented the U.S. government, stated, "they [Microsoft] have control of the evidence, that's what matters." Keshner, *supra* note 49.

102. Transcript of July 31 Order, *supra* note 11, at 69 ("In my view, also, the argument that the documents are not Microsoft's documents but the documents of its customers has been waived because it was not argued below."). By "below," Chief Judge Preska refers to the fact that Microsoft did not bring up this argument in their briefs to Magistrate Judge Francis and therefore cannot attempt to argue such points for the first time on appeal to the District Court, based on FED. R. CRIM. P. 59. Levine, *supra* note 21 (citing JOHN K. RABIEJ, 28 MOORE'S FEDERAL PRACTICE: CRIMINAL PROCEDURE § 659.11 (2014)). Levine makes the argument that the district court misapplied the Federal Rules of Criminal Procedure, finding that Microsoft should have had the right to object to the Magistrate Judge's order with "sufficient specificity so as reasonable to alert the district court of the true grounds of its objections." *Id.* Whether or not Microsoft could make such an argument to highlight the discrepancy that exists when applying the BNS Control Test to private emails of Microsoft customers, as opposed to Microsoft's accounting records, was not part of the court's analysis and not a focus of this Note. However, the lack of discussion of this potentially important distinction illustrates future difficulties companies will face in interpreting the consequences of the Microsoft Order. The result in this case may be an unwarranted extension of the BNS doctrine. *Id.* This was the first time the BNS doctrine had been applied to a warrant. *Id.* The question still remains how far the BNS doctrine of "control" reaches.

103. Transcript of July 31 Order, *supra* note 11, at 69–70.

Congress did intend the statute to apply extraterritorially if need be.[104] The court recognized the presumption against extraterritorial application of domestic laws unless there existed explicit congressional authorization.[105] However, the court held that because Congress was aware of the BNS cases, which were decided between 1982 and 1984, when it passed the SCA in 1986, following the canons of statutory construction, it was aware of the existing case law when it passed the SCA.[106] Therefore, if Congress knew of the existence of the BNS precedent, it would have drafted the statute to apply to information or documents located outside the United States so that the statute coincided with the then-contemporary (and recent) legal precedent of the BNS holding.[107]

C. EXTRATERRITORIAL "SEARCH AND SEIZURE" UNDER THE SCA

Beyond the issue of "control," Microsoft also argued it still should not be forced to disclose their customers' private e-mails because doing so would be authorizing an extraterritorial "search and seizure" warrant without the consent of the Irish government.[108] Microsoft contended that SCA warrants under § 2703 are confined to the borders of the United States. Specifically, Microsoft was adamant that the disclosure of its customers' private e-mails equated to a "search and seizure", analogous to that of a government search of the contents of a postal carrier's customers package.[109] According to Microsoft, the SCA does not explicitly permit extraterritorial seizures of private e-mails of this nature (or any nature to be exact).[110] In addition, such extraterritorial application of the SCA without the explicit consent of the Irish government or courts would violate international law and foreign policy.[111]

To counter, the U.S. government argued that even though the e-mails were located on servers in Ireland, since Microsoft could access the e-mails domestically, there was no actual extraterritorial application of the SCA

104. Keshner, *supra* note 49.

105. *See* Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010).

106. Keshner, *supra* note 49. *See generally* Karl N. Llewellyn, *Remarks on the Theory of Appellate Decision and the Rules of Canons About How Statutes are to be Construed*, 3 VAND. L. REV. 395 (1950); Levine, *supra* note 21. Levine finds this interpretation contentious because of the apparent conflict regarding the reach of the BNS doctrine, including whether the BNS doctrine applies to warrants, a company's business records, or also extends to its customers as well. *Id.*

107. Keshner, *supra* note 49.

108. Falcone, *supra* note 58.

109. *Id.* ("Microsoft analogized to a situation in which the government could subpoena a courier service to disclose records of where it shipped a customer's package, 'but any government-directed exploration of a package's contents would be a search because it would invade the reasonable expectation that sealed contents will remain private.' Microsoft's Reply in Support of Objections (Docket No. 70), at 4.").

110. *Id.*

111. Levine, *supra* note 21, at 2.

warrant.[112] Instead, due to the previously stated "hybrid" construction of the SCA warrant under § 2703,[113] it was the subpoena, not the warrant, that required Microsoft to obtain the e-mails from its data servers in Ireland and bring them to the United States.[114] The warrant part of the SCA only came into action once the e-mails were already within the United States; it addresses concerns over a private users' "reasonable expectation of privacy as to their emails."[115] Therefore, under a subpoena, Microsoft must produce evidence or information to the court within its "possession, custody, or control regardless of the location of that information," including the e-mails in question.[116]

Ultimately, the court determined there was no extraterritorial "search and seizure" under the SCA in this case.[117] Instead, the U.S. government was merely requiring a U.S. company subject to the jurisdiction of the United States, to produce electronic information within its control within the United States. The fact that the electronic information was located aboard was coincidental and non-determinative.[118] The court referred to § 442(1)(a) of the Restatement (Third) of Foreign Relations as dispositive because it allows courts or agencies in the United States, when "authorized" by statute or rule of the court, "[to] order a person subject to its jurisdiction to produce documents, objects or other information relevant to an action or investigation, *even if the information or the person is in possession of the information outside the United States*."[119] Therefore, according to the court, this "authorization" to order the production of the Microsoft e-mails comes from the SCA.[120]

---

112. *Id. See also* Falcone, *supra* note 58 ("In the government's view, no extraterritoriality issue is implicated here because the SCA is being applied solely to a US company within US territory. Per the government, '[a]n SCA warrant does not criminalize or regulate any conduct in a foreign country; it merely compels the provider receiving the warrant to disclose responsive records within its control to law enforcement agents located in the United State.' Government's Opposition to Microsoft's Objections (Docket No. 60), at 18.").

113. The SCA "hybrid" procedure noted previously in Magistrate Judge Francis's order. *In re* Warrant I Mag. J., *supra* note 5, at 471.

114. Levine, *supra* note 21.

115. Levine, *supra* note 21 (referencing potential Fourth Amendment conflicts resulting from the disclosure of third party private communications by an ISP to the U.S. government).

116. *In re* Warrant I Mag. J., *supra* note 5, at 472.

117. As the court concluded, "this was not extraterritorial application of United States law[,]" but instead, "[the] intrusion on the foreign sovereign" was "incidental at best." Transcript of July 31 Order, *supra* note 11, at 69.

118. *Id.* ("The result of that finding is that the production of that information is not an intrusion on the foreign sovereign. It is incidental at best.").

119. Keshner, *supra* note 49 (emphasis added). *See also* Transcript of July 31 Order, *supra* note 11, at 69 (citing RESTATEMENT (THIRD) OF FOREIGN RELATIONS § 422(1)(a)).

120. Levine notes that although the court does not explicitly say that this "authorization" comes from the SCA, it can be assumed that the court was referring to the SCA when quoting the relevant Restatement (Third) section. Levine, *supra* note 21.

D. MLAT TREATIES AND INTERNATIONAL COOPERATION IN CRIMINAL PROCEEDINGS

Microsoft argued that extraterritorial application of the SCA violated international law and foreign policy.[121] Specifically, it was referring to the fact that the United States was bypassing the traditional international procedure for exchange of documents and evidence between foreign nations. Microsoft argued that the proper avenue for the U.S. government to retrieve evidence located in Ireland is through the appropriate Mutual Legal Assistance Treaty (MLAT)[122] or through some sort of mutual cooperation between the U.S. and Irish governments.[123]

Traditionally, MLATs provide for the cooperation between signatory nations in criminal matters and proceedings, including the exchange of evidence and information during a criminal investigation.[124] For the purpose of this case, the United States and Ireland signed an agreement in which they agreed to provide mutual assistance in criminal proceedings and investigations, including the production of "documents, records, and articles of evidence;"[125] and the execution of requested "searches and seizures."[126] When, for example, the U.S. government wants to ask for the production of evidence located in Ireland that the United States cannot otherwise reach through existing legislation, the United States could put forth a request for the desired information or evidence to the Irish government.[127] In this request, the U.S. government shall describe the evidence, subject matter and nature of the investigation, and purpose for which the evidence is sought.[128] The request then goes through the Irish government, and if the request is accepted, it is processed under Irish law.[129] This means Ireland has the authority to issue orders deemed necessary to execute the request, either by subpoena, search warrant, or any other necessary order.[130] Additionally, if Ireland feels the execution of the request would interfere with Irish criminal investigations, or similar legal proceedings, Ireland has the right to postpone or alter the execution subject to its conditions.[131]

---

121. Falcone, *supra* note 58.
122. *See generally* U.S.-Ire. MLAT, *supra* note 20.
123. Falcone, *supra* note 58.
124. *In re* Request from United Kingdom to Treaty Between Gov't of United States & Gov't of United Kingdom on Mut. Assistance in Criminal Matters in the Matter of Dolours Price, 685 F.3d 1, 9 (1st Cir. 2012), *cert. denied sub nom.* Moloney v. United States, 133 S. Ct. 1796 (2013) ("The United States has entered into a number of mutual legal assistance treaties ('MLATs') which typically provide for bilateral, mutual assistance in the gathering of legal evidence for use by the requesting state in criminal investigations and proceedings.").
125. U.S.-Ire. MLAT, *supra* note 20, art. 1(2)(b).
126. *Id.* art. 1(2)(f).
127. *Id.* art. 4.
128. *Id.*
129. *Id.* art. 5. *See also id.* art. 14 (regarding "Requests for Seizures").
130. U.S.-Ire. MLAT, *supra* note 20, art. 5.
131. *Id.* art. 5(4).

Microsoft contends that extraterritorial application of the SCA allows the United States to bypass its MLAT obligation to Ireland and to obtain e-mails without going through the proper request channels.[132] According to Microsoft, the United States avoided asking for permission to obtain e-mails held within Irish borders altogether and instead, demanded Microsoft to produce the e-mails without Irish consent.[133] In response, the U.S. government claimed that nowhere is there a law that mandates the U.S. government to obtain evidence located in foreign nations through the MLAT process when other legal measures exist to appropriately obtain that evidence.[134] More importantly, the U.S. government argued that the MLAT process was, if anything, an impractical method of obtaining the pertinent evidence in the ongoing investigation.[135]

Ultimately, the court affirmed the Magistrate Judge's opinion that it made little sense to require the U.S. government go through the U.S.-Irish MLAT process.[136] Chief Judge Preska agreed with Magistrate Judge Francis that in drafting the SCA, Congress likely did not intend the U.S. government go through the time consuming and inefficient MLAT process to obtain overseas documents and information located on domestic ISPs.[137] The court found reliance on MLAT process alone was not necessary, as the process is excessively dependent on mutual cooperation between nations who could have varying political and judicial agendas, which runs counter to the time sensitive nature of ongoing criminal investigations.[138]

E. AN OUTLOOK TOWARDS THE SECOND CIRCUIT APPEAL

After the district court rejected Microsoft's challenge to the SCA warrant, Microsoft stated it would not fully comply with the warrant until at

---

132. Editorial, *Adapting Old Laws to New Technologies: Must Microsoft Turn Over Emails on Irish Servers?*, N.Y. TIMES (July 27, 2014), http://www.nytimes.com/2014/07/28/opinion/Must-Microsoft-Turn-Over-Emails-on-Irish-Servers.html?_r=0.

133. Falcone, *supra* note 58. *See also* Government's Brief In Support of the Magistrate Judge's Decision to Uphold a Warrant Ordering Microsoft to Disclose Records Within Its Custody and Control at 21–22, *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) [hereinafter Brief for Government] ("There is nothing in international law that requires the Government to use a Mutual Legal Assistance Treaty ('MLAT') to obtain evidence (particularly from a U.S. provider) located in a foreign country when other lawful means of obtaining the evidence are available. Nor do the specific MLATs the United States has signed with Ireland and the European Union contain any such requirement.").

134. The U.S. government uses the phrase "other lawful means of obtaining the evidence," referring to lawfully using the SCA to acquire the private e-mails in question as opposed to the U.S.-Ire. MLAT. Brief for Government, *supra* note 133, at 21–22.

135. The U.S. government reiterated its argument previously made before Magistrate Judge Francis in the initial proceeding against requiring the use of the U.S.-Ire. MLAT. *In re* Warrant I Mag. J., *supra* note 5, at 474–75.

136. *See* Keshner, *supra* note 49.

137. *See id.*

138. *Id.*

least appellate review had occurred.[139] Microsoft agreed to be held in contempt for its non-compliance with the court-ordered SCA warrant in order to appeal to the U.S. Court of Appeals of the Second Circuit without delay.[140] Microsoft made clear its intent to appeal as soon as possible.[141] Both parties have filed briefs with the Court of Appeals.[142]

IV. MICROSOFT'S COMPLIANCE PROBLEMS AS CONSEQUENCE OF THE EXTRATERRITORIAL APPLICATION OF THE SCA

The district court's approval of the SCA warrant has significant implications on Microsoft and other major U.S. Technology Companies going forward.[143] Microsoft's compliance with the SCA warrant may satisfy U.S. law, but may simultaneously violate the laws of a foreign nation, such as Ireland. This places Microsoft, and other U.S. Technology Companies, in the precarious situation of trying to determine which laws reign supreme. Additionally, the SCA warrant imposes the privacy laws of the United States on a foreign citizen in a foreign country, particularly egregious if the Microsoft user whose email account is under investigation is not a U.S. citizen. The SCA warrant throws the jurisdictional reach over electronic information into disarray and makes it difficult for U.S. Technology Companies to construct compliance policies.

As a result, this Part examines various challenges Microsoft and other U.S. Technology Companies face to set their privacy and business policies in response to the extraterritorial application of the SCA warrant. In

---

139. Michael Lipkin, *Microsoft Admits Contempt, Sets Up Appeal On Email Warrant*, LAW360 (Sept. 8, 2014), http://www.law360.com/articles/575248/microsoft-admits-contempt-sets-up-appeal-on-email-warrant.

140. The two parties (the United States government and Microsoft) disagreed regarding the correct "path" to appeal and are hotly contesting it now. *See* Zach Wittaker & Larry Seltzer, *Microsoft Refuses to Comply After Judge Revives Overseas Data Search Warrant*, ZDNET (Aug. 31, 2014), http://www.zdnet.com/article/microsoft-refuses-to-comply-after-judge-revives-overseas-data-search-warrant/. Procedurally, Microsoft had to admit to contempt so the order was final and subject to appellate review. *See* Rory Carroll, *Judge May Hold Microsoft in Contempt After Refusal to Hand Over Foreign Data*, THE GUARDIAN (Sep. 3, 2014, 3:08 PM), http://www.theguardian.com/technology/2014/sep/03/microsoft-contempty-court-judge-data-dispute. Ultimately, Microsoft agreed to be held in contempt instead of appealing the contempt order so that it could appeal the actual SCA warrant order without delay. *See* Lipkin, *supra* note 139; Bob Van Voris, *Microsoft Agrees to Contempt to Speed E-Mail Case Appeal*, BLOOMBERG NEWS (Sept. 8, 2014), http://www.bloomberg.com/news/2014-09-08/microsoft-agrees-to-contempt-to-speed-e-mail-case-appeal.html.

141. *See* Van Voris, *supra* note 140.

142. *See generally* Brief for Appellant, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985 (2d Cir. 2015), *available at* http://justsecurity.org/wp-content/uploads/2015/03/Microsoft-Opening-Brief-120820141.pdf. *See also generally* Brief for the United States of America, *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985 (2d Cir. 2015), *available at* http://justsecurity.org/wp-content/uploads/2015/03/GOVT-BRIEF.pdf.

143. *See* Levine, *supra* note 21.

particular, this Part looks at the Irish, and more broadly E.U., reaction to the SCA warrant and the economic implications on U.S. Technology Companies therefrom.

A. IRELAND'S REACTION TO THE SCA WARRANT IN ITS BACKYARD

The district court's approval of the Magistrate Judge's extraterritorial SCA warrant has stirred debate in Ireland over the legitimacy of U.S. procedural power to obtain evidence beyond its jurisdiction.[144] The Irish government has expressed concern over the United States' motion to directly obtain e-mails located on servers in Dublin, Ireland.[145] Over the years, Ireland has made itself an attractive site for U.S. Technology Companies to place their European headquarters.[146] Many of the United States' top technology companies, including Microsoft, have used Ireland as a location to host substantial data "server farms" (also known as data centers)[147] for their respective global data storage networks.[148] The fact that Ireland is commonly used as a station for data centers only heightens the tension between the United States and Irish government over the application of the SCA.

In response to the Microsoft warrant, Ireland's Prime minister of data protection, Dara Murphy, made clear that he found the United States' extraterritorial reach "objectionable," noting that the proper avenue to obtain the e-mails was through the established U.S.-Irish MLAT.[149] Murphy stated that Ireland was open to complying with the United States' request for the e-mails.[150] However, since the United States decided to bypass the bilateral agreement established by the U.S.-Irish MLAT,[151] questions of exactly who owns the Microsoft e-mail contents have arisen, including

144. *See Ireland Voices 'Serious Concern' over U.S. Order on Microsoft Emails*, U.K. REUTERS (Sept. 4, 2014, 1:05 PM), http://uk.reuters.com/article/2014/09/04/uk-usa-microsoft-emails-ireland-idUKKBN0GZ1CE20140904.

145. *See id.*

146. *See id.*

147. A "server farm" is defined as "a group of servers in one location connected by a network." Steven R. Swanson, *Google Sets Sail: Ocean-Based Server Farms and International Law*, 43 CONN. L. REV. 709, 714 (2011). With the expansion of cloud technology, global "server farms" have expanded in popularity among U.S. tech companies. This allows users, including individual customers and companies at large, to store what was once local computer data on "remotely-located computer servers" around the world. *Id.*

148. Tech companies such as Microsoft and Google. *See* REUTERS, *supra* note 144; Henry McDonald, *Ireland is Cool for Google as Its Data Servers Like the Weather*, THE GUARDIAN (Dec. 22, 2014), http://www.theguardian.com/technology/2012/dec/23/ireland-cool-google-data-servers-weather.

149. *See* REUTERS, *supra* note 144.

150. *See id.*

151. Although the U.S. government has argued that the U.S.-Ire. MLAT is not a mandatory procedural process. Brief For Government, *supra* note 133, at 21–22.

whether these e-mails are under the jurisdiction of the Irish government.[152] In addition, the question of ordering Microsoft to produce e-mails located on servers in Ireland violates Irish law.[153] The U.S. government contended that Microsoft failed to state any international law that would be violated by the SCA warrant's order to produce the relevant e-mails.[154] Furthermore, the crux of the U.S. government's argument was that not only will there be no violation of international law, but in fact the SCA warrant "does not involve an attempt to exercise control over foreign territory,"[155] and therefore, Microsoft's practical and jurisdictional limitation arguments are void. Although the U.S. government's argument has merit, there are obvious extraterritorial implications this ruling has on Ireland, Microsoft, and beyond.[156]

In Ireland, the Irish Data Protection Acts of 1988 and 2003 oversees the regulatory protection of data that is processed or controlled within Ireland.[157] These acts prohibit the transfer of personal data from Ireland to outside the "European Economic Area" unless adequate protections to personal privacy are made by the recipient nation.[158] The acts contain certain exceptions for the allowance of the transfer of personal data outside of the European Area for reasons of "'legal obligation' or 'necessary for the administration of justice.'"[159] Such provisions could legitimize the SCA's extraterritorial application in Ireland and its adherence to Irish law.[160] Although many legal experts and ex-lawmakers[161] have openly denounced

---

152. Jennifer C. Archie & Ulrich Wuermeling, *Microsoft Stands Up in Court for European Privacy Rights?*, LEXOLOGY (Sept. 8, 2014), http://www.lexology.com/library/detail.aspx?g=0f15ad1b-cd22-4f3b-929b-43e5cdcead6a.

153. *Id.*

154. Brief For Government, *supra* note 133, at 21–22.

155. *Id.* at 20. Backing for this statement comes from the SCA's "hybrid" part subpoena /part warrant construction, along with the fact that the evidence requested is electronic and therefore can be acquired and viewed domestically, with no need for federal agents to seize the e-mails abroad. *See In re* Warrant I Mag. J., *supra* note 5, at 475–77.

156. O'Connor, *supra* note 24.

157. *Id.* ("The Irish Data Protection Acts 1988 and 2003 seek to regulate the collection, processing, use and disclosure of data relating to individuals that is processed or controlled in Ireland.").

158. *Id.*

159. *Id.*

160. In contrast, Michael McDowell, a former Irish Attorney General and now pre-eminent barrister before the Irish Supreme Court, has argued that such exceptions are "*only lawful where such disclosure is required or mandated by reference to Irish law and is subject to the jurisdiction and control of the Irish courts*." *Id.* (emphasis in original).

161. Michael McDowell stated that "MLAT was the appropriate procedural forum for the transfer to take place." *Id.* Dara Murphy, the Irish Minister of State at the Department of the Taoiseach and Foreign Affairs with Special Responsibility for European Affairs and Data Protection, claimed that "compliance with the warrant may result in Microsoft, and any other U.S. companies with operations in the E.U. which are served with such warrants in the future, being in breach of the Acts and the EU Data Protection Directive, stating that '*this would create significant legal uncertainty for Irish and EU consumers and companies regarding the protection of their data which, in this digital age, is everyone's most valuable asset*.'" *Id.* (emphasis in original).

the United States' infringement on Irish soil, it is unlikely that "Irish privacy law will be decisive in the Microsoft case,"[162] at least as it pertains to the upcoming appeal.

Although the United States' disregard of Irish law may not be decisive in determining the issuance of the SCA warrant, Ireland's reaction has economic and policy implications on Microsoft in its global compliance.[163] If Microsoft has to produce the evidence for the U.S. government, others will question Ireland's ability to protect customer's data (both foreign and domestic) from government intrusion. In addition, the order could inhibit Microsoft's expanding cloud computing global network.[164] Ireland has already filed an amicus brief in support of Microsoft over this order.[165] Irish customers would be tempted to avoid using Microsoft and other U.S. Technology Companies to store their information to avoid U.S. government intrusion in their data.[166] It is unclear what Microsoft could do to its business models and privacy policies to give Irish customers clear assurances when their private electronic data and information will or will not be subject to existing U.S. privacy legislation.[167]

B. ON A BROADER SCALE: TENSIONS RISE BETWEEN THE EUROPEAN UNION AND THE UNITED STATES

The district court's decision to uphold the SCA warrant raises tensions between the United States and foreign nations, in particular those within the E.U., when it comes to the U.S. surveillance of international data security and privacy protections.[168] The NSA WikiLeaks/Snowden scandal is only but a recent memory, especially for those of the E.U.[169] The E.U. is still hesitant of the United States' unrefined and mostly undefined Internet privacy policies after the NSA's "sweeping surveillance was legalized when

---

162. Archie & Wuermeling, *supra* note 152.

163. *See generally* O'Connor, *supra* note 24.

164. *See id.*

165. Mark Scott, *Ireland Lends Support to Microsoft in Email Privacy Case*, N.Y. TIMES (Dec. 24, 2014, 5:44 AM), http://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/?_r=1. In its brief, Ireland states it would be pleased to expeditiously consider a request for the private e-mails should the United States make one through the U.S.-Ire. MLAT. Brief of Ireland, as Amicus Curiae Supporting Appellants at 4, *In re* Warrant to Search a Certain E-Mail Account Controlled & Operated by Microsoft Corp., No. 14-2985-cv (2d Cir. 2015).

166. O'Connor, *supra* note 24.

167. The existing U.S. legislation being the SCA and the vague framework the court had to work with in applying the dated statute to the realities of modern technology and global data networks. *See generally* Kattan, *supra* note 4.

168. Falcone, *supra* note 58 ("In allowing the magistrate judge's ruling to stand, the federal district court may have inadvertently heightened tensions between the US government and privacy advocates, and raised even more challenges for US service providers as they seek to negotiate a path between compliance with US law and the privacy demands of both their customers and authorities outside the US, particularly in Europe.").

169. *See* Levs & Shoichet, *supra* note 19.

Congress passed the USA PATRIOT Act."[170] After documents were revealed that exposed the NSA's surveillance was not only of suspected terrorists, but of communications between Americans and roughly thirty-five world leaders,[171] the N.S.A's "PRISM Programme continues to haunt the principles of data protection across Europe."[172] Therefore, the district court's approval of the SCA warrant only increases the E.U.'s skepticism of U.S. data privacy laws and heightens their fear of privacy violations by the United States.

Certain E.U. nations have taken, or have threatened to take, significant action in response to the district court's ruling.[173] For example, the German government has already publically stated that it will refuse to use any U.S. company for data storage unless the Microsoft warrant is overturned.[174] Germany could be the first of many countries to shy from using U.S. data companies for data storage to avoid privacy risks as a consequence of the SCA's extraterritorial reach.[175] For Microsoft, this would be increasingly problematic both for their international cloud network and business outlook.[176] Microsoft stands to lose an entire nation's worth of revenue that cannot easily be replaced. More importantly, such a loss would enable foreign competitors to gain stronger positions in the cloud industry, as foreign customers elect to use non-U.S. Technology Companies to store their wealth of electronic information due to U.S. privacy concerns. It remains unclear whether there is anything Microsoft could do on its own to repair its business relationship with Germany and other E.U. nations from a privacy policy perspective as the law currently stands.[177] The Managing Director of Microsoft Germany has been busy at work trying to come up with solutions should the warrant be upheld on appeal.[178] However, no solution would completely alleviate the United States' ability to request

---

170. Elizabeth Atkins, *Spying on Americans: At What Point Does the NSA's Collection and Searching of Metadata Violate the Fourth Amendment?*, 10 WASH. J.L. TECH & ARTS 51, 55 (2014).

171. *See* James Ball, *NSA Monitored Calls of 35 World Leaders After US Official Handed Over Contacts*, THE GUARDIAN (Oct. 25, 2013), http://www.theguardian.com/world/2013/oct/24/nsa-surveillance-world-leaders-calls.

172. O'Connor, *supra* note 24.

173. *Id.*

174. *Id.*

175. At this point, it would not be surprising if such an international reaction occurred since it seems unlikely for the order to be overturned by the Second Circuit under the existing legal framework and legislation. It would then only be upon Congressional amendment to the SCA that the United States could assuage European nations to do business with U.S. technology companies for data storage, because these companies would be unable to promise data security abroad. *See* Levine, *supra* note 21.

176. *See* O'Connor, *supra* note 24.

177. *See id.*

178. *See id.*

data stored on Microsoft servers in Germany, unless the data was completely separated from the United States.[179]

Beyond Germany, other European nations, including Ireland, have formally requested that the European Commission examine whether the SCA warrant violates any E.U. data protection laws.[180] U.S. Technology Companies have also pushed the E.U. to investigate whether the district court's ruling has violated E.U. data privacy laws as well. The amount of legal uncertainty the extraterritorial application of the SCA creates is alarming both to foreign nations and domestic technology companies alike.[181] The fact that neither the E.U. Commission nor U.S. companies know if E.U. data protection laws have been violated only highlights the inherent difficulty in finding an international solution should the SCA warrant be approved on appeal.

Currently, it is not yet clear if the district court's order and magistrate judge's warrant under the SCA forces Microsoft to violate any E.U. privacy laws.[182] Microsoft has previously argued before both the magistrate judge and district court judge that the proper channel to obtain the e-mails was through the bilateral U.S.-Irish MLAT.[183] However, as previously noted, this is a flawed argument as the U.S.-Irish MLAT is neither mandatory nor persuasive.[184] Looking at the E.U.'s data protection laws directly does not

---

179. Managing Director of Microsoft Germany, Dr. Christian Illek, has stated that Microsoft is

> considering the possibility of working with partners to develop a cloud data centre based in Germany, with the aim of alleviating national concerns over cyber security. According to Dr. Illek, Microsoft is testing the idea of a 'German cloud system', where data could be hosted by a partner company (rather than a Microsoft Group company) but not be subject to US law.

Id. This is similar to the ideas of "cloud localization," a concept China and Russia have begun to establish. *See* Allison Grande, *Apple's China Data Storage Portends Localization Movement*, LAW360 (Aug. 22, 2014, 5:52 PM), http://www.law360.com/articles/569841/apple-s-china-data-storage-portends-localization-movement.

180. *See* Jennifer Baker, *Call the Commish! Ireland Dragged into Microsoft Dispute Over Alleged Drug Traffic Data*, THE REGISTER (Nov. 19, 2014), http://www.theregister.co.uk/2014/11/19/call_the_commish_ireland_dragged_into_alleged_drug_traffickers_microsoft_data_dispute/.

181. Mary Minihan, *Microsoft Data Case May Have 'Very Serious' Implications—Minister*, IRISH TIMES (Sept. 3, 2014, 6:02 PM), http://www.irishtimes.com/news/politics/microsoft-data-case-may-have-very-serious-implications-minister-1.1916834 (statement of Irish Minister of State for Data Protection Dara Murphy) ("This would create significant legal uncertainty for Irish and EU consumers and companies regarding the protection of their data which, in this digital age, is everyone's most valuable asset.").

182. *See* Baker, *supra* note 180.

183. *See generally In re* Warrant I Mag. J., *supra* note 5; Transcript of July 31 Order, *supra* note 11; *In re* Warrant II C.J., *supra* note 11.

184. *In re* Warrant I Mag. J., *supra* note 5, at 374–75 ("Moreover, nations that enter into MLATs nevertheless generally retain the discretion to decline a request for assistance."). *See also* Brief for Government, *supra* note 133, at 21–22 ("There is nothing in international law that requires the Government to use a Mutual Legal Assistance Treaty ('MLAT') to obtain evidence

help much either. In 1995 the European Community (EC) "attempted to harmonize data protection laws in order to secure approval from EC member states through the EC Data Protection Directive."[185] Initially, EC member states that had "historically high data protection standards," were hesitant to approve the legislation.[186] In response, the EC Data Protection Directive included a general ban on processing and transferring personal data outside the European Economic Area (EEA), unless a limited number of exceptions applied.[187] Therefore, before the E.U. could transfer personal data outside the EEA, the recipient nation must have established "adequately protective privacy laws."[188]

U.S. privacy laws do not pass this criterion.[189] However, data transfer between the U.S. and E.U. was still necessary, and therefore the two agreed to establish the Safe Harbor Privacy Principles[190] to allow U.S. companies a method to certify compliance with E.U. privacy standards to enable the transfer.[191] Microsoft is certified under Safe Harbor Principles to transfer personal data between the E.U.[192] In addition, Microsoft's terms of use for its e-mail platform, Outlook.com, "explicitly reserve[s] the right to provide user data in order to satisfy applicable law, regulation, legal process or governmental requests."[193] To add to the confusion, some have claimed that the private e-mails, should they be produced and transferred under the SCA warrant, would not be transferred under Safe Harbor Principles.[194] Therefore, further investigation is necessary to determine Microsoft's liability through compliance with the SCA warrant.

Most importantly, Microsoft and other U.S. Technology Companies are in the near impossible situation of sifting through vague domestic and international legislation in the attempt to create a definitive and clear privacy policy to calm frustrated customers and avoid violating either

---

(particularly from a U.S. provider) located in a foreign country when other lawful means of obtaining the evidence are available.").

185. Lothar Determann & Robert Sprague, *Intrusive Monitoring: Employee Privacy Expectations Are Reasonable in Europe, Destroyed in the United States*, 26 BERKELEY TECH. L.J. 979, 1023 (2011) (citing Council Directive 95/46/EC, 1995 O.J. (L 281) 31, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do? uri=CELEX:31995L0046:EN:HTML).

186. *Id.* at 1024.

187. *Id.* at 1024 n.233 ("The European Economic Area (EEA) is comprised of the twenty-seven EU member states, plus three more—Iceland, Liechtenstein, and Norway—which agreed under a separate treaty to adopt certain EU laws. *See* Agreement on the European Economic Area (EEA), 1994 O.J. (L 1) 3 (May 2, 1992), available at http://ec.europa.eu/world/agreements/prepareCreateTreatiesWorkspace/treatiesGeneralData.do? step=0&redirect=true&treatyId=1.").

188. Kesan et al., *supra* note 4, at 419.

189. *Id.*

190. Commission Decision 2000/520/EC, 2000 O.J. (L 215) 7, *available at* http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32000D0520&from=en.

191. Kesan, et al., *supra* note 4, at 420.

192. Archie & Wuermeling, *supra* note 152.

193. *Id.*

194. O'Connor, *supra* note 24.

foreign or domestic law.[195] U.S. technology and cloud providers would "need to promptly review their business models and engage with data protection regulators, at least to the extent they host data, including personal data, in the EEA on behalf of third parties . . . ."[196]

However, what makes this alteration to U.S. Technology Companies' business models even more difficult is the fact that the SCA's approval is based on the vague and overly expansive BNS doctrine.[197] The district court's ruling "creates significant risk for any company subject to U.S. jurisdiction by weakening its ability to protect its customers' information, abolishing distinctions between a company's own business records and its customers' private correspondence, and subjecting companies to potential sanctions for violating privacy laws of the countries in which they locate their data centers."[198] The BNS doctrine simply does not afford enough clarity to the present case to allow data storage companies, such as Microsoft, to make the proper adjustments to their policies to allow them to sufficiently comply both domestically and internationally.[199] It is important, however, to note that this problem does not lie with the court's ruling and interpretation of the law. Rather, the problem stems from the out-of-date SCA, which courts are now forced to stretch to apply to the modern advancements of global cloud network technology.[200]

It is therefore the recommendation of this Note to update the SCA to reflect the globalized reality of today's data sharing capabilities.[201] The district court's interpretation of the SCA in *In re Warrant* is the most recent example of the statutes ineffectiveness in promoting consistent and comprehensible application and compliance. The problem lies in Congress, not the courts. Congress needs to decide whether it wants to treat electronic evidence in the same fashion as traditional physical evidence. If electronic evidence were treated similarly, physical location of the data server would determine the nation having jurisdiction over that information. Therefore, evidence physically held in foreign nations would be beyond the reach of U.S. warrants and would require the cooperation of foreign authorities. U.S. Technology Companies would surely prefer this method of procedure. However, the inefficiencies mentioned by the U.S. government of MLATs and the need to strike a balance between privacy and public safety make this an unlikely solution. Instead, amending the MLAT process to create a more streamlined system of processing cross-border electronic evidence

195. *Id.*
196. *Id.*
197. *See* Levine, *supra* note 21.
198. *Id.*
199. *Id.*
200. *See* Kattan, *supra* note 4, at 617.
201. Kesan et al., *supra* note 4, at 401 ("The status of the SCA is problematic because much of the language is very unclear or outdated and interpretations of the statute by courts have varied significantly.").

requests that still respects the distinguishable privacy rights of separate nations would be a good bridge-gap for the SCA. This would allow Congress some time to contemplate and effectuate a more significant overhaul of the legislation overseeing electronic information in the near future.

V. ECONOMIC CONSEQUENCES ON MICROSOFT AND THE REST OF THE U.S. DATA SERVICE INDUSTRY

The district court's approval of the SCA warrant not only creates compliance problems on a legislative level for Microsoft, but also creates very real economic implications for Microsoft's expansion as a business and the evolution of the cloud industry as a whole.[202] Cloud technology has erupted over the past few years and has been the new focal point for data storage global strategies for technology companies.[203] Cloud technology promotes a global network of shared data that is transferrable beyond borders.[204] This inherent transferability and expansive structure that permeates through cloud technology is exactly what makes the industry so profitable and important for the future of the technology industry.[205] Studies have shown "digital trade has increased the U.S. GDP by 3.4 to 4.8 percent and created up to 2.4 million jobs."[206] A McKinsey Report also estimated that "improved use of data generates as much as $5 trillion in additional economic value each year in seven industries alone."[207]

In particular, the "transatlantic data flows" between the United States and E.U. have become increasingly important for the progress of national economies and the prominent U.S. Technology Companies that supply both the United States and E.U. with data networks. Microsoft is one of the

---

202. *See* O'Connor, *supra* note 24 ("The ramifications of this decision for technology companies threatens the growth of the global cloud model . . . ."); Denys Emmert, *DOJ Overreach Could Kill The Digital Economy*, THE DAILY CALLER (Oct. 23, 2014, 1:23 PM), http://dailycaller.com/2014/10/23/doj-overreach-could-kill-the-digital-economy/.

203. Robinson, *supra* note 1, at 1199.

204. *See generally* K. Senathipathi, et al., *A Cross Border Access to Data Stored In the Cloud*, 2 INT'L J. OF ADVANCED RES. IN COMPUTER ENGINEERING & TECHNOLOGY 2707 (2013). *See also* Robinson, *supra* note 1, at 1203 ("This [cloud storage] business model is expanding rapidly as users and providers realize its benefits . . . . The liability of the technology and its growing acceptance by consumers and service providers offer powerful evidence that a lasting technological and societal shift is underway.").

205. *See* Joshua Meltzer, *The Importance of the Internet and Transatlantic Data Flows for U.S. and EU Trade and Investment* (Brookings, Working Paper 79, 2014), *available at* http://www.brookings.edu/~/media/Research/Files/Papers/2014/10/internet%20transatlantic%20data%20flows%20meltzer/internet%20transatlantic%20data%20flows%20version%202.pdf.

206. *Id.* at 1.

207. Emmert, *supra* note 202 (citing JAMES MANYIKA ET. AL., MCKINSEY GLOBAL INST., OPEN DATA: UNLOCKING INNOVATION AND PERFORMANCE WITH LIQUID INFORMATION (2013), *available at* http://www.mckinsey.com/insights/business_technology/open_data_unlocking_innovation_and_performance_with_liquid_information).

preeminent U.S. Technology Companies.[208] U.S. Technology Companies are at the forefront of the global market and their growth depends on the ease of electronic information transfer between data servers around the world without jurisdictional hindrance.[209] E-mails, like the ones in contention in the *In re Warrant* case,[210] are stored as part of these cloud computing services, which topped business expenditures for over $174 billion dollars in 2014 and is expected to increase exponentially in the upcoming years.[211] Therefore, Microsoft and other U.S. Technology Companies have much to lose financially from "foreign retaliation" against the extraterritorial application of the SCA.[212]

As previously noted, U.S. Technology Companies are still reeling from the backlashes of the NSA privacy scandal.[213] Edward Snowden, a previous NSA employee, released information that the NSA had been collecting mass electronic surveillance data from companies like Microsoft, Apple, Google, and Facebook to spy on foreign governments.[214] If foreign nations view U.S. Technology Companies as unofficial extensions of the U.S. government, U.S. companies risk huge losses in business from overseas customers.[215] Foreign customers neither want to be associated with a government known for extensive privacy violations, nor subject to invasive U.S. privacy laws simply by being a customer of a U.S. corporation. Germany has been outright with its discontent with American data companies and has already refused to use Microsoft or any other U.S. data company for its data services, unless the SCA warrant is overturned.[216] China has expressed its intention to begin a data localization movement, in

---

208. *See* Meltzer, *supra* note 205. *See also Cloud Solutions*, MICROSOFT PARTNER NETWORK, https://mspartner.microsoft.com/en/us/Pages/Solutions/microsoft-cloud-solutions.aspx (last visited Feb. 28, 2015) (stating experts expect Microsoft public IT cloud services industry to reach over $107 billion by 2017); Motley Fool, *supra* note 13 ("Microsoft is betting its future on the cloud. Its [sic] cloud computing platform, Azure, is expected to become the backbone of Windows 10.").

209. Steve Pociask, *DOJ's 2-Million-Jobs Mistake*, THE HILL (Sept. 30, 2014, 10:00 AM), http://thehill.com/blogs/congress-blog/judicial/219033-dojs-2-million-job-mistake.

210. *See In re* Warrant I Mag. J., *supra* note 5.

211. Pociask, *supra* note 22, at 4 (citing data from the U.S. Census Bureau, U.S. Bureau of Economic Analysis, as of September 4, 2014).

212. Pociask, *supra* note 209.

213. Matt Day, *Microsoft's Rivals Become Its Allies in Overseas Email Warrant Case*, SEATTLE TIMES (Dec. 13, 2014), http://seattletimes.com/html/businesstechnology/2025232338_microsoftirishserverxml.html?syndication=rss ("Facing skeptical customers at home and abroad in the wake of Edward Snowden's disclosures about the extent of the government's reach into the Internet, Microsoft, and peers such as Google and Facebook, have taken the opportunity to speak up.").

214. Motley Fool, *supra* note 13.

215. *Id.*

216. *See* O'Connor, *supra* note 24 ("The German Government has stated it will not store data with US cloud providers unless the decision is overturned."). *See also* Motley Fool, *supra* note 13 ("In June, the German government replaced Verizon with Deutsche Telekom, citing surveillance concerns presumably related to the Angela Merkel phone-hacking scandal.").

which it would only rely on data servers physically located in China.[217] Neither of these reactions is particularly surprising considering the continued skepticism of U.S. foreign surveillance policies, and it is entirely possible that this international backlash will continue.

For companies like Microsoft, who "generate a substantial portion of their revenue overseas," and rely on the cloud for the future success of their tech business, the foreign backlash against the extraterritorial application of the SCA is a financial nightmare.[218] The extraterritorial application of the SCA is seen as a U.S. invasion of personal privacy abroad.[219] If foreign nations are purposefully avoiding using American companies such as Microsoft, it will directly inhibit Microsoft's cloud data network expansion. In addition to Microsoft losing customers worldwide, investors are going to be more skeptical about the company's future in dealing with these increasing compliance issues and customer losses, and may be less likely to invest in Microsoft's future on the open market.[220] This amount of uncertainty, as a result of extraterritorial application of the SCA, frightens U.S. Technology Companies about their economic future. [221]

VI. FUTURE LEGISLATION AND CONSIDERATIONS – INTRODUCTION OF THE LEADS ACT TO SENATE

In reaction to the extraterritorial application of the SCA in *In Re Warrant of a Certain E-mail Account Controlled and Maintained by Microsoft Corporation,*[222] several members of Congress have already introduced a new bill to the Senate floor to quell domestic and international reactions to the warrant and to begin the process of amending the SCA.[223] The new bill, entitled the LEADS Act,[224] looks to "preclude the use of U.S. warrants to obtain communications content stored outside the [United States] unless the content is in the account of an American."[225] Therefore, in order for the United States to be able to force Microsoft to disclose private e-mails located on servers abroad through the use of a judicial warrant, the customer or user of those e-mails must be a U.S. citizen.[226] The goal of this

217. *See* Grande, *supra* note 179.
218. Motley Fool, *supra* note 13.
219. Pociask, *supra* note 209.
220. Motley Fool, *supra* note 13.
221. *See id.*
222. *See generally In re* Warrant I Mag. J., *supra* note 5; Transcript of July 31 Order, *supra* note 11; *In re* Warrant II C.J., *supra* note 11.
223. Introduced by Sen. Orrin Hatch (R-UT), Sen. Chris Coons (D-DE), and Sen. Dean Heller (R-NV). The LEADS Act, *supra* note 26.
224. *Id.* ("To amend title 18, United States Code, to safeguard data stored abroad from improper government access, and for other purposes.").
225. 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/.
226. *See id.*

Act is to help deal with the foreign reaction to the SCA warrant and soften fears of foreign citizens of being subject to U.S. privacy invasion.

As previously discussed, a clear indication of Congress's extraterritorial intent is worriedly missing from SCA itself.[227] The language of the SCA is vague at best, and its legislative history does not give insight as to whether Congress intended the SCA warrant to apply so broadly when it was first drafted in 1986. The LEADS Act seeks to clarify Congress's intention of the extraterritorial application of the SCA and to limit the judicial warrant's international scope and reach. The courts should not be forced to interpret the SCA as it is currently written with as much discretion as they are forced to use since the statute is dated and presently insufficient. The reactions from U.S. Technology Companies and nations abroad from the current SCA warrant interpretation shows that clarification and limitations on the United States' extraterritorial warrant powers on electronic data is necessary going forward.[228] Whether the LEADS Act clarifies the SCA enough or whether it will be passed by the Senate and ratified at all remains to be seen.

In addition, the LEADS Act seeks to improve the MLAT process. The U.S. government's decision to seek an SCA warrant for the e-mails in Ireland, as opposed to following MLAT procedure for production, was largely based on the MLAT's inefficiencies, especially in matters of high security.[229] The LEADS Act would "require the Department of Justice to create an online intake form through which foreign governments could request mutual legal assistance, and it would permit the DOJ to give preference to requests made on-line."[230] The LEADS Act seeks to modernize the MLAT process so that countries can more easily obtain evidence abroad through their respective treaties.[231] However, such computerization of the MLAT requires money, and this is subject to the politics of obtaining sufficient federal funding.

In theory, modernizing the MLAT process would be incredibly beneficial to the United States. Ideally, the United States should be utilizing the MLAT to seek assistance in obtaining evidence located in foreign nations which are parties to such treaties. . This pertains to electronic evidence, including e-mails, as well. The MLAT approach is currently the "best way to accommodate the interests of two governments when one country seeks data stored in another country."[232] By making an MLAT request, the United States is being open about its intentions to obtain electronic information stored abroad. With today's technology and the ease of transferring and storing electronic information throughout the world, this

227. *In re* Warrant I Mag. J., *supra* note 5, at 472.
228. *See* Nojeim, *supra* note 225.
229. *See In re* Warrant I Mag. J., *supra* note 5, at 473.
230. Nojeim, *supra* note 225.
231. *See* The LEADS Act, *supra* note 26, § 4 ("Mutual Legal Assistance Treaty Reforms").
232. *Id.*

formal request, although time-consuming, respects a nation's boundaries and ensures private personal information is obtained with consent.

At the same time, there is merit to the U.S. government's argument that the current MLAT process is slow and subject to political objectives that may not conform to time sensitive investigations of international matters of concern.[233] It is evident Microsoft and Ireland denounce the U.S. government's alleged bypass of the U.S.-Irish MLAT.[234] Although the U.S.-Irish MLAT's purpose is "to improve the effectiveness of the law enforcement authorities of both countries in the investigation, prosecution, and prevention of crime through cooperation and mutual legal assistance in criminal matters,"[235] and, traditionally, is the process by which the U.S. government would obtain evidence located in Ireland through a domestic warrant, the U.S. government's arguments for efficiency in relation to criminal investigation has legitimate backing in today's post-9/11 era. Criminal investigations on high security matters, such as drug enforcement or terrorism, need to run smoothly and efficiently because time of the essence. There is no reason to bog down investigations where critical evidence is located abroad and risk losing valuable intelligence due to another nation's potential political goals that may be in opposition with the ongoing U.S. investigation in sending the evidence in a timely manner.

Additionally, the current extraterritorial application of the SCA warrant does not allow the U.S. government to obtain electronic information from anyone for any reason. There are constitutional measures in place, in particular the Fourth Amendment that requires the U.S. government to show before a judge probable cause for issuing the SCA warrant. To establish probable cause, the U.S. government must establish the individual in question is suspected of illegal activity and that obtaining the e-mails located abroad is vital to the ongoing investigation.[236] The extraterritorial application of the SCA would not unduly expand the power of the U.S. government to freely obtain any electronic information from anybody it so chooses. However, there are serious problems with allowing the U.S. government to bypass the MLAT process altogether. Instead, the U.S. government has chosen to take an expansive interpretation of a dated statute to allow the U.S. government to obtain electronic evidence without the consent or even request of the foreign nation where the electronic evidence is stored.[237] It was able to do this because the SCA is so vague to begin with and therefore can be construed widely. The courts had little choice but to

233. *See In re* Warrant I Mag. J., *supra* note 5, at 474–75 (quoting Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PENN. L. REV. 373, 409 (2014)).

234. *See* O'Connor, *supra* note 24.

235. *See* U.S.-Ire. MLAT, *supra* note 20, and discussion *supra* Introduction.

236. *See In re* Warrant I Mag. J., *supra* note 5, at 470, 471.

237. *See id.* at 467, 477.

uphold the extraterritorial application of the SCA warrant based on current legislation.

Improving the MLAT process under the LEADS Act is a great start to establishing a procedure for the United States to obtain electronic evidence stored abroad. It allows the already established legal channels for exchanging evidence between nations to proceed as intended, while also accounting for the problems that nations, such as the United States, now face when investigating and prosecuting criminal matters due to the ubiquitous presence of electronic information. It remains to be seen if such an online MLAT database can be created. More importantly, the bill itself is the foundation for a global conversation about how to deal with the transfer of electronic data stored around the world for criminal investigations.[238] Customers of U.S. Technology Companies seek certain assurances of the privacy of their information that they store on cloud servers. In turn, U.S. Technology Companies must be able to provide customers with reasonable expectations of their privacy rights. In addition, U.S. Technology Companies need clear and precise compliance standards so as not to violate domestic and international law. All of these factors conflict with the uncertainty created by the extraterritorial application of the current SCA.[239] The global discussion must continue in order to help find the balance between the needs of the U.S. government's ability to efficiency investigate criminal matters in conjunction with U.S. Technology Companies needs of continued financial success and privacy protections.

CONCLUSION

This Note concludes that extraterritorial application of the SCA is too vague and inconclusive for U.S. Technology Companies to properly construct legitimate privacy policies for their customers and thereby threatens their economic growth. Congress must amend the SCA to not only clarify Congress's intentions for extraterritorial application of the SCA warrant, but also to make sure there are safeguards against excessive international application of the SCA warrant so that foreign law is not violated or disturbed through cross-border criminal procedure. The extraterritorial application of the SCA warrant places U.S. Technology Companies that rely on worldwide cloud storage networks, such as Microsoft, in danger of losing huge sums of business due to an ambiguous and dated statute.[240] In addition, the extraterritorial interpretation of the SCA further strains the United States' international relations with foreign

238. Nancy Scola, *Senate's New Overseas-Email Protection Act Gets Mixed Reviews*, WASH. POST (Sept. 18, 2014), http://www.washingtonpost.com/blogs/the-switch/wp/2014/09/18/senates-new-overseas-email-protection-act-gets-mixed-reviews/.

239. *See* Pociask, *supra* note 22.

240. *See* Day, *supra* note 213.

nations, especially those in the E.U., when it comes to data protection and privacy rights.

The introduction of the LEADS Act into the Senate floor is a start to clarifying and narrowing the scope of the SCA.[241] However, the LEADS Act is only the beginning of what is a long process of overhauling data privacy statutes written during the Internet's mainstream conception in the Regan-Era. Beyond making congressional statutes more relevant to modern times, however, the U.S. government must also assist U.S. Technology Companies by updating its own cross-border processes as well. The U.S. government should take advantage of the technological advances available in order to improve the efficiency of the international exchange of online information and evidence for criminal proceedings. The world will only continue to become more and more globally dependent. Issues of cross-border conflict over the exchange of online information will be a continuously heated issue of contention unless steps are taken now to catch up to the realities of the global infrastructure of electronic information.

Ned Schultheis[*]

241. *See* Nojeim, *supra* note 225.

* B.A., Tulane University, 2011; J.D. Candidate, Brooklyn Law School, 2016. I want to sincerely thank everyone on the *Brooklyn Journal of Corporate, Financial & Commercial Law* for their selfless hard work in preparing this Note for publication. Special thanks to Liana-Marie Lien and Peter Flynn for their guidance, support, and dedication. I am incredibly indebted to the Honorable Loretta A. Preska, for giving me the chance of a lifetime last summer and exposing me to the arguments that inspired this Note. Finally, I want to thank all my friends and family, for without them, I would not be where I am today.