Where in the World is Your Data? Who Can Access It?

Katherine Grabar *

TABLE OF CONTENTS

* J.D. Candidate, The George Washington University Law School, May 2018. B.A., Political Science and Law, History, and Culture, University of Southern California, May 2015. The author would like to thank James Brecher for teaching her about legal writing, analysis, and advocacy. She dedicates this note to her parents and grandparents who gave her the instrumental gift of education.

I. INTRODUCTION

People take pictures on their Apple iPhones, save documents to Google Drive, or send emails using Microsoft's Outlook.com. Companies, like Microsoft, Apple, and Google, make these services available to their users and store the user-created data on their own servers, as opposed to on the device used to create the work product.[1] This storage function is called the "cloud."[2] Customers using the cloud can access their data from any Internet-enabled device and share the data with others while preventing data loss.[3] The cloud is a large number of grounded servers located across the globe, and in the United States alone, the cloud is responsible for two percent of the country's electricity usage.[4] The servers powering the cloud must be stored at a location with a low temperature because if they overheat, the servers will crash.[5] When these servers, hosted in data centers, overheat, users' devices cannot access the content they need.[6] In response, Microsoft developed Project Natick to solve this problem of overheated servers by operating data centers in the ocean.[7] The ocean keeps the data centers cool so consumers can access their data without delay, and the technology companies furnishing the servers save money on their electricity bill.[8]

The Stored Communications Act ("SCA"), which is part of Title II of the Electronic Communications Privacy Act ("ECPA"), is the "primary law governing government and private actor access to our stored online communications" written in 1986.[9] Courts differ on how to interpret the anachronistic statute, some choosing to protect electronic communications that did not exist at the time of the SCA's passage, like data stored in the

---

1. *See* David Goldman, *What is the cloud?*, CNN (Sept. 14, 2014, 9:05 AM), http://money.cnn.com/2014/09/03/technology/enterprise/what-is-the-cloud/index.html [https://perma.cc/3T7L-QZBU]. Businesses use similar storage services for medical and financial data, work product, and trade secrets. *See* Reuven Choen, *The Could Hits the Mainstream: More than Half of U.S. Businesses Now Use Cloud Computing*, FORBES (Apr. 16, 2013, 9:23 AM), https://www.forbes.com/sites/reuvencohen/2013/04/16/the-cloud-hits-the-mainstream-more-than-half-of-u-s-businesses-now-use-cloud-computing [https://perma.cc/Z2AF-AE6].

2. *See* Jess Fee, *The Beginner's Guide to the Cloud*, MASHABLE (August 26, 2013), https://mashable.com/2013/08/26/what-is-the-cloud/ [https://perma.cc/W2UL-ZG4G].

3. *See* Nicole A. Ozer & Chris Conley, *Cloud Computing: Storm Warning for Privacy?*, ACLU NORTHERN CAL. (Jan. 2010), https://www.aclunc.org/sites/default/files/privacy_and_free_speech_it's_good_for_business,_2nd_edition.pdf [https://perma.cc/RV44-RR99].

4. Goldman, *supra* note 1.

5. *See* John Markoff, *Microsoft Plumbs Ocean's Depths to Test Underwater Data Center*, N.Y. TIMES (Jan. 31, 2016), https://www.nytimes.com/2016/02/01/technology/microsoft-plumbs-oceans-depths-to-test-underwater-data-center.html [https://perma.cc/H2W9-D2LA].

6. *See id.*

7. *Id.*

8. *Id.*

9. RICHARD M. THOMPSON II & JARED P. COLE, CONG. RESEARCH SERV., R44036, STORED COMMUNICATIONS ACT: REFORM OF THE ELECTRONIC COMMUNICATIONS PRIVACY ACT 1 (2015).

cloud, while others fail to modernize their interpretation.[10] Without legal protection, the technological process will be inhibited if consumers and businesses do not have confidence that their data will be secure in new technologies like the cloud.[11]

The Second Circuit recently grappled with the SCA's applicability to cloud data stored in Dublin in a Microsoft data center.[12] The Court denied the government's search warrant application to access data in the Dublin data center because the SCA did not specifically mention that the law governs data extraterritorially.[13] An obsolete SCA thus produces an environment where online cloud data does not possess the same privacy protections as data stored on a home computer or in a filing cabinet.[14]

Congress has repeatedly failed to update the SCA to govern privacy rights in the massive amounts of data consumers store in the cloud.[15] This creates an even larger challenge when applied to the underwater data centers Microsoft is developing. The Second Circuit held that the United States does not have jurisdiction to access data that is not stored domestically.[16] Accordingly, the United States likely does not have jurisdiction over data stored at sea in places like underwater data servers in Microsoft's Project Natick.

Congress must amend the SCA to protect privacy interests and empower the government to engage in effective investigative searches. Law enforcement, armed with a search warrant, needs the ability to access the data of United States citizens stored on domestically and internationally. Companies that operate their own cloud services should not be able to store data wherever they please, based on a company policy designed to avoid potential government seizure. An updated Stored Communications Act should include: (i) jurisdiction to search overseas data of United States citizens; (ii) jurisdiction to search data physically stored in the United States; and (iii) a warrant and notice requirement for search of any electronic

---

10. *Compare* Theofel v. Farey-Jones, 359 F.3d 1066, 1075-76 (9th Cir. 2004) (concluding messages stored on a web server are included in the definition of electronic communications of the Stored Communications Act), *with* Steve Jackson Games, Inc. v. U.S. Secret Serv., 36 F.3d 457, 461-62 (5th Cir. 1994) (holding once communications are received they are no longer in electronic transmission) ("[T]he ECPA's legislative history makes it crystal clear that Congress did not intend to change the definition of "intercept" as it existed at the time of the amendment.").

11. *See* Elizabeth MacDonald, *NSA Leaks Slam Could Computing Industry*, FOX BUSINESS (Aug. 9, 2013), http://www.foxbusiness.com/politics/2013/08/09/nsa-leaks-slam-cloud-computing-industry.html [https://perma.cc/MDS5-279B] (revealing the billions of dollars potentially lost from the fallout of NSA spying programs).

12. *See* Peter J. Henning, *Microsoft Case Shows the Limits of a Data Privacy Law*, N.Y. TIMES (July 18, 2016), https://www.nytimes.com/2016/07/19/business/dealbook/microsoft-case-shows-the-limits-of-a-data-privacy-law.html [https://perma.cc/XM38-4XGH].

13. *See* Brian Jacobs, *The Microsoft Warrant Case: Unintended Consequences of the Second Circuit's Ruling*, FORBES (Aug. 2, 2016, 5:04 PM), https://www.forbes.com/sites/insider/2016/08/02/the-microsoft-warrant-case-unintended-consequences-of-the-second-circuits-ruling/#3b3b5ca52f28 [https://perma.cc/D2MM-FT3Z].

14. *See* Ozer & Conley, *supra* note 3.

15. *See* THOMPSON & COLE, *supra* note 9, at 8-15.

16. *See* Microsoft Corp. v. United States, 829 F.3d 197, 222 (2d. Cir. 2016).

communications. These solutions are necessary to create clear procedures for searches and search warrant applications to protect law enforcement investigations, individual privacy, and the business of technology companies.

This Note proceeds in three parts. Part II outlines the text and legislative history of the Stored Communications Act and the Second Circuit's interpretation of the SCA in *Microsoft Corp. v. United States*. Part III addresses the consequences of inaction through a review of the lack of law enforcement search tools abroad without extraterritorial application of the SCA, Microsoft's development of underwater data servers, and a review of proposed and unsuccessful legislation to amend the SCA. Part IV proposes jurisdictional and privacy amendments to the SCA that provide law enforcement with the ability to search data with a warrant based on probable cause for electronically stored data of any United States citizen or data geographically stored within the United States. This proposed jurisdictional power is balanced with a warrant requirement for any stored data and notification requirement to any user whose data is seized.

II. THE STORED COMMUNICATIONS ACT: AN OUTDATED STATUTE APPLIED TO A MODERN-DAY DISPUTE

The Stored Communications Act was enacted to protect electronic communications from unreasonable searches and seizures.[17] However, the law has not been substantively updated in the thirty years since it was introduced.[18] An outdated law, in combination with developing technology, yields uncertain privacy protection for individuals over data stored using cloud technology.[19] The SCA inhibits an individual's attempt to protect data and law enforcement's endeavors to engage in lawful searches of data to investigate unlawful activity.[20] The Second Circuit interpreted the Stored Communications Act and concluded that the law does not authorize application of a United States search warrant to data stored overseas.[21] According to the Second Circuit's interpretation, the statute failed to grant law enforcement the power to search data overseas because there was no explicit provision discussing extraterritorial application or cloud data.[22] This outdated statute creates ambiguity as to an individual's privacy rights such that a corporation's decision of where to store data determines whether the data receives Fourth Amendment protections.[23]

17. *See* THOMPSON & COLE, *supra* note 9, at 1.
18. *See* Henning, *supra* note 12.
19. *See* Ozer & Conley, *supra* note 3, at 7.
20. *Id*.
21. *Microsoft*, 829 F.3d at 220.
22. *Id.* at 206, 211.
23. *Id.* at 224 (Lynch, J. concurring).

A. The Problem: The Outdated Text of the Stored Communications Act

Congress enacted the ECPA and the SCA to extend the application of the Fourth Amendment privacy right to electronic communications.[24] Before the statute, there was no explicit regulation governing who could access electronically stored data and when access was granted.[25] The statute outlines with whom network providers may share a customer's data, since customers may not store their own data when using electronic services.[26] The SCA instructs providers of electronic communication services on when they can share customers' information and communications[27] and dictates the proper standards for law enforcement to gain access to this data.[28] Service providers undertake the obligation to protect users and their data, with the exception of subpoenas and warrants based on probable cause.[29] The statute "allows law-enforcement agencies to obtain stored e-mail, account records, or subscriber information from a service provider."[30] Even though the statute has not been meaningfully updated since its passage, courts now interpret the SCA to govern electronic content, such as emails, YouTube videos, Facebook messages, and metadata related to Internet transactions.[31]

Under the SCA, an administrative subpoena can grant the government access to basic subscriber and transactional information.[32] However, law enforcement needs more than just a subpoena to access the actual content of stored communications because the SCA requires a warrant for "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less."[33]

---

24. *See* Melissa Medina, *The Stored Communications Act: An Old Statute for Modern Times*, 63 AM. U.L. REV. 267, 276 (2013).

25. *Id.* at 274-76.

26. *Id.* at 277.

27. According to the ECPA and the SCA, an electronic communication is any communication that is not a wire or oral communication. For example, an email is an electronic communication. DANIEL J. SOLOVE & PAUL M. SCHWARTZ, PRIV., INFO., AND TECH. 149 (3d. ed. 2011). Federal courts corroborate this interpretation. *See Theofel*, 359 F.3d 1066 (recognizing storage of copy of emails falls within jurisdiction of the SCA); Fraser v. Nationwide Mutual Insurance Co., 352 F.3d 108 (3d Cir. 2003) (examining emails stored via backup methods).

28. *See* THOMPSON & COLE, *supra* note 9, at 3. Congress differentiated between the two categories of data because in 1986, users would download the emails onto their own machines instead of storing them with third-party providers and the copies the provider had were akin to business records. Serrin A. Turner, *Are Changes in Store for the Stored Communications Act?*, 2-6 PRATT'S PRIV. & CYBERSECURITY L. REP. 04 (2016).

29. *See* Samantha V. Ettari et al., *Second Circuit Rules That the U.S. Government Cannot Use a Search Warrant to Access Overseas Data*, 277-279 PRATT'S PRIV. & CYBERSECURITY L. REP. 03 (2016); Nora Ellingsen, *The Microsoft Ireland Case: A Brief Summary*, LAWFARE (July 15, 2016, 10:34 AM), https://www.lawfareblog.com/microsoft-ireland-case-brief-summary [https://perma.cc/6C5M-86V4].

30. Jessica R. Herrera-Flanigan, CYBERCRIME AND JURISDICTION: A GLOBAL SURVEY 317 (Bert-Jaap Koops & Susan W. Brenner eds., 2006).

31. THOMPSON & COLE, *supra* note 9, at Introduction.

32. 18 U.S.C. § 2703(c)(2).

33. *See* § 2703(a).

For any communications older than 180 days, the government must notify the subscriber or customer, or obtain a warrant.[34] Classifications within the statute dictate different protections for the same email if it is in transit, opened and stored in remote storage, stored on a home computer, unopened and stored for 180 days or less in remote storage, or in remote storage for more than 180 days while unopened.[35]

B. The Stored Communications Act: Too Old to Regulate the Microsoft Cloud and the Data Within It

On December 4, 2013, Magistrate Judge James C. Francis IV granted the United States government's warrant, in accordance with the SCA, for data stored by the Microsoft Corporation ("Microsoft") for a criminal narcotics investigation.[36] Microsoft stored most of the data relating to the government's request in one of its data centers in Dublin, and the rest in the United States.[37] Believing the warrant only authorized seizure of data located in the United States, Microsoft only provided the data stored domestically.[38] Judge Francis disagreed with Microsoft's interpretation, and decided that seizure of any relevant data was proper because the location where the government would review the data was "the relevant place of seizure," not the location the data was stored.[39] The District Court denied its motion to quash the government's warrant, and as a result, Microsoft appealed the decision to the Second Circuit Court of Appeals.[40]

The government's search of this data was problematic because data moves between Microsoft's servers in data centers around the world based on Microsoft's policy of placing data in a data center closest to a user's country code set by the user's stated preference.[41] In *Microsoft*, the country code dictated the data move to Microsoft's Dublin data center.[42] Once the data was transferred, all the data left remaining on the original server, here, a United States server, was non-content email information, some of the user's address book, and basic account information.[43]

The Second Circuit found that Congress enacted the SCA in order to provide the privacy protections of the Fourth Amendment to users of electronic communication services.[44] The technological knowledge Congress

34. § 2703(b)(1)(A)-(B).

35. *See* Electronic Communications Privacy Act (ECPA), ELECTRONIC PRIV. INFO. CENTER, https://epic.org/privacy/ecpa/ [https://perma.cc/Z8XG-QXEH], (last visited Dec. 14, 2016) (demonstrating a warrant is required to access an email in transit while an opened email stored remotely only requires a subpoena).

36. *Microsoft*, 829 F.3d at 203; Ettari et al., *supra* note 29, at 03.

37. *See Microsoft*, 829 F.3d at 204.

38. *Id*.

39. *Id.*

40. *Id*. at 200.

41. *Id.* at 203.

42. *Id*.

43. *Id*.

44. *Id.* at 206; *see also* S. COMM. ON JUDICIARY, ELECTRONIC COMMUNICATIONS PRIVACY ACT OF 1986, S. REP. NO. 99-541, at 5 (1986).

possessed thirty years ago when it passed the ECPA is considerably different from today because of the great advances in the industry.[45] "[A] globally-connected Internet available to the general public for routine e-mail and other uses was still years in the future when Congress first took action to protect user privacy."[46]

The Second Circuit interpreted Supreme Court precedent to mandate that unless Congress specifically states otherwise, there is a presumption against applying United States law extraterritorially.[47] The SCA makes no such mention of extraterritorial application.[48] Even without the explicit mention of extraterritorial application, the Second Circuit noted that the "far-reaching state court authority" laid out in the SCA would inevitably conflict with foreign laws if applied outside of the United States.[49]

Drawing on this interpretation, the Court found that, "[b]ecause the content subject to the [w]arrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States."[50] The lack of explicit authorization for such action caused the Second Circuit's reversal of the District Court.[51] Microsoft would have to inevitably interact with a non-domestic data server in order to execute the search warrant.[52] The Second Circuit held that Microsoft adequately complied with the search warrant for the data stored domestically and had no further obligations to law enforcement.[53]

Judge Lynch wrote a concurring opinion to illustrate the practical consequences of the Court's decision and the apparent need to modernize the SCA.[54] The opinion emphasized how the court's holding was not actually a win for privacy interests generally; rather, only those who lived abroad or claimed to live abroad gained any additional protection from the court's holding.[55] This application of the SCA permits an American user to misrepresent where she is located solely to evade potential seizure and it likewise permits Microsoft and companies like it to move data in order to evade government searches.[56] According to Judge Lynch, a "sensible" resolution of the court's decision would be nuanced, accounting for more than

45. *See Microsoft*, 829 F.3d at 205-06.

46. *Id*. at 206 (citing Craig Partridge, *The Technical Development of Internet Email*, IEEE ANNALS OF THE HIST. OF COMPUTING 3, 4 (Apr.-June 2008)).

47. *See Microsoft*, 829 F.3d at 210 (citing Morrison v. National Australia Bank Ltd., 561 U.S. 247 (2010)). The Supreme Court recognizes that Congress typically legislates on domestic matters rather than foreign ones and that Congress is a governmental entity more fit to make decisions regarding international relations than are the courts. *Microsoft*, 829 F.3d at 210.

48. *Id*. at 211. *Contra* Weiss v. National Westminster Bank PLC, 768 F.3d 202, 207 & n.5 (2d Cir. 2014); United States v. Weingarten, 632 F. 3d 60, 65 (2d Cir. 2011).

49. *See* Microsoft, 829 F.3d at 211.

50. *Id.* at 220.

51. *Id*. at 222.

52. *Id*. at 220.

53. *Id*. at 222.

54. *Id*. (Lynch, J., concurring).

55. *Id.* at 224. (Lynch, J., concurring).

56. *Id.* at 230 (Lynch, J., concurring).

just what Congress anticipated in 1986.[57] "Our decision today is thus ultimately the application of a default rule of a statutory interpretation to a statute that does not provide an explicit answer to the question before us."[58]

III. *MICROSOFT CORP. V. UNITED STATES*: ONE OF MANY REASONS THE STORED COMMUNICATIONS ACT REQUIRES AN UPDATE

Without a law to authorize searches extraterritorially, United States law enforcement can only obtain overseas data by a mutual legal assistance treaty.[59] International law governs the parameters of a search for a law enforcement investigation and inhibits law enforcement from doing their job.[60] Underwater data centers will only worsen the ambiguity surrounding searches since these centers are not necessarily located in any jurisdiction to which a mutual legal assistance treaty would apply. Law enforcement, under the SCA interpretation in *Microsoft*, would not have any recourse to search the data. Congressional attempts to amend the SCA in recent legislative sessions have been unsuccessful and Congress has been unable to create complete and effective solutions to any of these issues.[61]

A. Ramifications of Microsoft Corp. v. United States Beyond One Search Warrant

The Second Circuit is one of many courts across the globe grappling with jurisdictional questions about electronically stored data.[62] Treaties and the lack thereof cause a "jurisdictional headache" for courts where companies like Microsoft have "headquarters in one country, servers in another, and users all around the world."[63] United States law enforcement and governmental entities have to submit a request to a country with which it in a mutual legal assistance treaty ("MLAT") and must follow the outlined

57. *See id*. at 231 (Lynch, J., concurring). *See also* Henning, *supra* note 12 (quoting the concurrence "[T]here is no evidence that Congress has ever weighed the costs and benefits of authorizing court orders of the sort at issue in this case").

58. *See Microsoft*, 829 F.3d at 232 (Lynch, J., concurring). Judge Lynch asserted at oral argument that it "would be helpful if Congress would engage" in the task of updating the statute, while acknowledging that speed is not Congress' strength. Alex Ely, *Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview*, LAWFARE (Sept. 10, 2015, 5:08 PM), https://www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview [https://perma.cc/CWX2-CXPA].

59. *See Microsoft*, 829 F.3d at 221.

60. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 409 (2014); *see also* U.S. Dep't of State, Treaties, Agreements and Asset Sharing (2014), https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm [https://perma.cc/GE6Q-YKRK].

61. *See* Kerr, *supra* note 60, at 373; *see, e.g.*, Email Privacy Act, H.R. 699, 114th Cong. (2015).

62. Kerr, *supra* note 60, at 376.

63. *Id*.

procedures.[64] The parties to the treaty consult with the Office of International Affairs at the Department of Justice to obtain data on a foreign server pursuant to the MLAT.[65] The MLAT does not necessarily describe the complete process; a combination of national laws govern the procedure.[66] United States law enforcement seeking the information is therefore at the mercy of the partner country to respond to the request, if the country responds at all.[67] If the country does respond, the typical international response takes months, not days.[68] The MLAT does not require a response when "the execution of such [a] request would be prejudicial to the state's security or public interest; the request relates to a political offense; there is an absence of reasonable grounds; the request does not conform to the MLAT's provisions; or the request is incompatible with the requested state's law."[69] Where the United States has not signed a MLAT with the country, the United States government has no formal way to conduct searches of data centers abroad.[70]

Certain countries who reject the MLAT approach mandate forced data localization to exercise control over data and ensure their own access by "requir[ing] the information service provider to build out a physical, local infrastructure in every jurisdiction in which it operates, increasing costs . . . for both providers and consumers."[71] However, these requirements are difficult to enforce and drive potential wrongdoers to engage in more secretive practices.[72] These policies can affect privacy, security, economic

64. *See* Microsoft, 829 F.3d at 221; Andrew Keane Woods, *Reactions to the Microsoft Warrant Case*, LAWFARE (July 15, 2016, 7:21 AM), https://www.lawfareblog.com/reactions-microsoft-warrant-case [https://perma.cc/GE7R-SZ27]. A MLAT is a bilateral agreement between the United States and another country to aid in criminal investigations. Thomas G. Snow, *Prosecuting White-Collar Crime: The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them*, 11 WM. & MARY BILL OF RTS. J. 209, 223-25 (2002).

65. *See* Herrera-Flanigan, *supra* note 30, at 324.

66. *See* Gail Kent, *The Mutual Legal Assistance Problem Explained*, CTR. FOR INTERNET AND SOC'Y BLOG (Feb. 23, 2015, 1:06 PM), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [https://perma.cc/A3VT-8K89].

67. *See* Susan W. Brenner et al., *Transnational Evidence Gathering and Local Prosecution of International Cybercrime*, 20 J. MARSHALL J. COMPUTER & INFO. L. 347, 384 (2002).

68. *See* United Nations Office on Drugs and Crime, Comprehensive Study of the Problem of Cybercrime and Responses to it by Member States, the International Community and the Private Sector, U.N. Doc. No. UNODC/CCPCJ/EG.4/2013/2 (Jan. 23, 2013), https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_E.pdf [https://perma.cc/36UV-PWWQ].

69. *See* Anupam Chander & Uyen P. Le, *Data Nationalism*, 64 EMORY L.J. 677, 734 (2015).

70. *See Microsoft*, 829 F.3d at 221. As of 2014, the United States only had mutual legal assistance treaties with 57 nations. *See* U.S. DEPARTMENT OF STATE, TREATIES, AGREEMENTS AND ASSET SHARING (2014), https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm [https://perma.cc/GE6Q-YKRK]. Ultimately this note focuses solely on the domestic statutory analysis and not the international framework. A larger discussion of law enforcement access to information on the international level would further delve into an MLAT and Privacy Shield discussion that would frankly overwhelm and distract from this note's purpose.

71. *See* Chander & Le, *supra* note 69, at 681.

72. *Id*. at 732.

development, international trade, and innovation.[73] MLATs reduce the risk of countries requiring data localization requirements and avoid an even bigger jurisdictional headache for extraterritorial data searches.[74]

B. Cloud Innovation: Microsoft Underwater Data Center

Many individuals already engage in most of their work through the cloud.[75] A majority of technology experts agree that most people will access and share information through cloud computing by 2020.[76] Webmail services, like that Microsoft provides, is one of the most prevalent of the cloud services offered.[77]

In order for customers to utilize email, engage in social networking, and stream video all while on the cloud, companies like Microsoft need data servers that do not overheat, and plenty of space to store the data servers.[78] If the servers reach too high of temperatures, they crash.[79] Current data centers are built far away from users and hubs because they require large spaces to be built and are costly to maintain.[80] Microsoft developed Project Natick to solve these problems; the Project aims to operate data centers in the ocean, possibly on the sea floor, or in containers beneath the surface and connected to land by a fiber-optic cable.[81] These aquatic data centers promise to transmit data faster than current data centers are capable of because "half of the world's population lives within 120 miles of the sea" so the data centers will be much closer to the users they serve.[82]

Microsoft engaged in a successful 105-day trial of a steel capsule containing a data center 30 feet underwater in the Pacific Ocean and 30 kilometers from shore.[83] The capsule was connected to land through a cable,

---

73. *Id*. at 681.

74. *See* Int'l Chamber of Commerce, *Using Mutual Legal Assistance Treaties (MLATs) To Improve Cross-Border Lawful Intercept Procedures* 3 (2012), https://www.iccwbo.be/wp-content/uploads/2016/03/20120912-ICC-policy-statement-on-MLAT.pdf [https://perma.cc/43HY-B4UB].

75. *See* Janna Anderson & Lee Rainie, *The future of cloud computing*, PEW RESEARCH CTR. (June 11, 2010), http://www.pewinternet.org/2010/06/11/the-future-of-cloud-computing/ [https://perma.cc/EAF8-HHFU].

76. *See id*.

77. *See id*.

78. *See* Markoff, *supra* note 5. Microsoft is not the only company innovating to decrease the burden of data storage; Nautilus Data Technologies is building the first commercial data center on water. *See* George Leopold, *Navy backs development of first 'data barge'*, DEFENSE SYSTEMS (Nov. 19, 2015), https://defensesystems.com/articles/2015/11/19/navy-nautilus-floating-data-barge.aspx [https://perma.cc/TRN9-HHFQ]. The company discussed the product and selling it to "the industry's leading technology companies." *Id*.

79. *See* Markoff, *supra* note 5.

80. *Id*.

81. *Id*.

82. *See* James Eng, *Project Natick: Microsoft Tests Putting Data Centers Under the Sea*, NBC NEWS (Feb. 1, 2016, 4:59 PM), https://www.nbcnews.com/tech/innovation/project-natick-microsoft-tests-putting-data-centers-under-sea-n508946 [https://perma.cc/S5MX-BU5M].

83. *See* Markoff, *supra* note 5.

which was then connected to the Internet to transmit data.[84] According to Microsoft, the results of the test run thus far are "promising."[85] Because of these promising results, Microsoft expects to develop underwater data centers that last up to five years without significant maintenance.[86] Microsoft engages in this innovation to respond to the increasing demand for mass amounts of data storage at a faster speed as opposed to the typical storage on a user's device.[87]

C. Congress' Lack of Impactful Action Leaves the SCA in the Twentieth Century

Congress first attempted to amend the ECPA and SCA in 2011 after technology companies, academics, and privacy advocates lobbied to communicate the importance of an update to the statutes.[88] The technology community recognized that, "the ECPA is an anachronistic statute, one ill-suited to contemporary law enforcement and global electronic communications."[89] Most Congressional proposals merely tinkered with the 1986 statute, even though the ECPA requires drastic reform to adapt to the changes in technology and the Internet since 1986.[90] Congress presented solutions by recommending a requirement for a warrant for any seizure regardless of the age of the communication, enforcement of a blanket prohibition on any voluntary disclosure of customer data, and a notice requirement for the customer's data searched by law enforcement.[91] No Congressional attempt, thus far, has been successful at achieving any meaningful change.[92] The following two attempts illustrate this lack of success and examine how the statutes could have held up in the *Microsoft* case instead of the archaic SCA.

The Email Privacy Act was the most successful Congressional attempt to amend the ECPA. The House Judiciary Committee unanimously voted it out of Committee and it passed the House of Representatives with unanimous approval as well.[93] Under the Act, the provider of an electronic communication service, the technology company and host of the cloud had to

---

84. *See Project Natick*, MICROSOFT, https://news.microsoft.com/natick/ [https://perma.cc/PA7J-9CX9] (last visited Dec. 13, 2016).

85. *See* Eng, *supra* note 82.

86. *See id.*

87. *See* Markoff, *supra* note 5.

88. *See* THOMPSON & COLE, *supra* note 9, at 8.

89. *See* Ely, *supra* note 58.

90. *See* Kerr, *supra* note 60, at 373, 375 (suggesting repeal of the ECPA and law to replace it).

91. *See* THOMPSON & COLE, *supra* note 9, at 8-15.

92. *Id*. at 8.

93. *See* Turner, *supra* note 28, at 04; Sophia Cope, *House Advances Email Privacy Act, Setting the Stage for Vital Privacy Reform*, ELEC. FRONTIER FOUND. (Apr. 27, 2016), https://www.eff.org/deeplinks/2016/04/house-advances-email-privacy-act-setting-stage-vital-privacy-reform [https://perma.cc/QXF3-F66F]; *see also* Eric Geller, *Major online privacy bill easily clears first vote in Congress*, THE DAILY DOT (Apr. 13, 2016, 12:00 PM), https://www.dailydot.com/layer8/email-privacy-act-house-judiciary-committee-passage/ [https://perma.cc/GEJ2-H2QJ].

disclose data "that is in electronic storage with or otherwise stored, held, or maintained" when law enforcement was armed with a proper warrant.[94] Any government search or seizure of emails required a search warrant; stored documents only required a subpoena.[95] However, the Email Privacy Act did not differentiate between emails and stored communications older or newer than 180 days, as the current SCA does, so any email search required a warrant.[96] If the government entity was a law enforcement entity, they had to give notice to the consumer if it accessed the consumer's data within ten days, and within three days for any non-law enforcement governmental entity.[97]

The Email Privacy Act would not have actually impacted the warrant requirement for data seizure if it had been enacted. Since the Sixth Circuit decided *United States v. Warshak* in 2010, the Department of Justice's policy already enforced a warrant requirement for electronic data stored with electronic service providers, regardless of the 180 and non-180 day requirements of the SCA.[98] Therefore, this change would have merely codified what the federal government was already doing, and thus maintained the status quo.[99] Modern email storage renders most emails stored in data centers older than 180 days anyway; for example, Google stores about 17,000 emails for the average Gmail user.[100] The notification requirements of three and ten days in the Act only notified a customer after data is seized.[101] Customers would be left to trust the technology company to fight for their rights because they have no recourse before the search occurs. The technology company only risks reputational harm if it does not fight for a customer's rights; for the customer, however, the damage caused could be loss of his confidential communications or work product, and the consequences could be his livelihood or even freedom.

Another Congressional attempt to reform the ECPA, The Law Enforcement Access to Data Stored Abroad Act, recognized the jurisdictional issue that created the holding of the *Microsoft* case, "[N]either ECPA nor subsequent amendments extended the warrant power of courts in the United States beyond the territorial reach of the United States."[102] According to the Act, the location of the data did not matter; instead, the government could properly obtain any data with an adequate warrant if it was for a United States'

94. *See* Email Privacy Act, H.R. 699, 114th Cong. § 3 (2015).

95. *See* Geller, *supra* note 93.

96. *See* THOMPSON & COLE, *supra* note 9, at 9.

97. *Id*. Law enforcement can request a notification delay of not more than 180 days; any other government entity can request a delay of no more than 90 days. *Id* at 10.

98. The Sixth Circuit held email accounts in the purview of third-party services have Fourth Amendment protections and require a warrant for seizure. *See* United States v. Warshak, 631 F.3d 266 (6th Cir. 2010); Turner, *supra* note 28, at 04.

99. *See id*.

100. *See* Mike Barton, *How Much Is Your Gmail Account Worth?*, WIRED (July 25, 2012), https://www.wired.com/insights/2012/07/gmail-account-worth/ [https://perma.cc/4S3K-RYVX].

101. *See* THOMPSON & COLE, *supra* note 9, at 10.

102. *See* Law Enforcement Access to Data Stored Abroad Act, S.2871, 113th Cong. § 2 (2014).

citizen.[103] But the court of proper jurisdiction would modify or vacate the warrant if the provider had to violate the laws of a foreign country by giving the United States government the data.[104] Congress recognized that service providers could store customer data in multiple locations and the user is not always in the same country as the data.[105] While the Act did not grant jurisdiction to law enforcement, it did allow the Department of Justice and United States Attorney General to streamline MLAT requests, inventory requests sent and received, and review the data of what is actually received and sent.[106] Unfortunately, the Law Enforcement Access to Data Stored Abroad Act never left the Senate Judiciary Committee.[107] Had the bill made it out of Committee, law enforcement, network providers, and individuals could have more clarity about what determined whether United States law enforcement could search their data. This law clearly allowed United States law enforcement to search the data of any United States citizen, regardless of where the data would be stored.[108] The Law Enforcement Access to Data Stored Abroad Act attempted to address the issue of jurisdiction in contention in *Microsoft*.[109] However, the Act only allows seizure of data of United States citizens subject to legal privacy regimes in other countries.[110]

IV. SUGGESTED AMENDMENTS TO MODERNIZE THE STORED COMMUNICATIONS ACT

The Internet of 1986 only slightly resembles the Internet used today.[111] The drafters of the SCA would not have contemplated regulating cloud storage as a means of storing mass amounts of user data because the public did not have universal access to the Internet in 1986.[112] Now with cloud data, electronic service providers can store customer data at their own discretion, to such an extreme that the data could be fragmented around the world and only legible with the assembly of every single piece.[113] Additionally, at the time of the SCA's enactment, the cost of electronic storage was too high to

103. *See id.*; *see also* Patrick Maines, *The LEADS Act and cloud computing*, THE HILL (March 30, 2015), http://thehill.com/blogs/pundits-blog/technology/237328-the-leads-act-and-cloud-computing [https://perma.cc/QG2L-EKS9].

104. *See* S.2871, 113th Cong. § 3 (2014).

105. *See* THOMPSON & COLE, *supra* note 9, at 14.

106. *See* S.2871, 113th Cong. § 4 (2014).

107. *See S.2871 - The Law Enforcement Access to Data Stored Abroad Act*, CONGRESS.GOV, https://www.congress.gov/bill/113th-congress/senate-bill/2871/committees?q=%7B%22search%22%3A%5B%22Law+Enforcement+Access+to+Data+Stored+Abroad+Act%22%5D%7D&r=1 [https://perma.cc/436J-LURK] (last visited Nov. 19, 2016).

108. *See* S.2871, 113th Cong. § 3 (2014).

109. *See* CONGRESS.GOV, *supra* note 107.

110. *See* THOMPSON & COLE, *supra* note 9, at 14.

111. *See* Kerr, *supra* note 60, at 376.

112. *See* Ellingsen, *supra* note 29.

113. *See* Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CON. L. HEIGHT. SCRUTINY 11, 20-21 (2012) (illustrating Google and Amazon's tendency to fragment consumer data).

contemplate regulating it.[114] In the thirty years since then, costs of storage plummeted and technology companies evolved to turn a profit by charging for electronic storage on their own servers.[115]

The Second Circuit reserved the issue of regulation of data in the cloud for Congress to resolve based on Supreme Court precedent and the lack of explicit law enforcement power to search data overseas in the SCA. Law enforcement does not have any domestic law that specifically guides them in searches of cloud data stored overseas.[116] Individuals are likewise left in the dark as to how the data they entrust to a third party will be stored and when it will be turned over to law enforcement. Network providers have to muddle through interpreting a twentieth century law in a twenty-first century technological world. Until Congress acts, the Supreme Court must grapple with the possible creation of a judicial solution to a legislative problem when *Microsoft* comes for argument before the Court.[117]

An underwater data center solution to the need for data storage can only exacerbate the demand for a legislative update to the SCA. At least with the data stored in Dublin, law enforcement could adhere to an MLAT to search the data.[118] For data stored at sea, there is no means to access the data.

These amendments focus on assuring an informed and consistent law for users and businesses located in the United States to solve the jurisdictional problems presented by the *Microsoft* case and Microsoft's underwater servers.[119] Any changes to the statute should also simplify the structure to enable it to evolve with developments of technology.[120]

A. First Proposed Amendment: United States Law Enforcement Has Jurisdiction Over United States Citizen's Data

United States privacy regulations should follow the data of a United States citizen, regardless of the data location.[121] This clear rule assures and informs United States users that their own domestic law would apply in any search and seizure scenario.[122] Making a citizen subject to the law of his or her own country makes logical sense and likely meets consumer expectations

114. *See* Kerr, *supra* note 60, at 376; *see also* R.J.T. Morris & B.J. Truskowsi, *The Evolution of Storage Systems*, 42 IBM SYS. J. 205, 205-06 (2003) (reviewing the development of electronic storage methods).

115. Kerr, *supra* note 60, at 376.

116. *See Microsoft*, 829 F.3d at 210

117. *See* Jose Pagliery, *Supreme Court to rule if Microsoft must turn over emails stored overseas*, CNN (Oct. 16, 2017, 10:17 AM), http://money.cnn.com/2017/10/16/technology/business/supreme-court-microsoft/index.html?sr=twtech101617supreme-court-microsoft0223PMVODtopLink&linkId=43551689 [https://perma.cc/G37X-J9RH].

118. *See Microsoft*, 829 F.3d at 221.

119. *See* Medina, *supra* note 24, at 292-93.

120. *See id.* at 292.

121. *See* Kerr, *supra* note 60, at 417.

122. *Id.*

since these laws were enacted by their own elected representatives.[123] Data of United States citizens should be subject to search by the United States according to United States law, even if it is stored abroad, as long as the warrant satisfies probable cause.

This proposed amendment would not be a new concept in Congress. The Law Enforcement Access to Data Stored Abroad Act proposed a similar requirement but allowed for other countries' laws to dictate whether the search could proceed.[124] The intent of a uniform rule is laudable, however, another country interfering with an investigation of a United States citizen by United States law enforcement only creates more ambiguity. The bureaucratic hold-up multiplies with the approach in the Law Enforcement Access to Data Stored Abroad Act because law enforcement must garner approval for the warrant and have the judge interpret the laws of the country in which the data is physically located to determine whether the search would be lawful.[125] A clear rule, free of any other country's privacy laws, will create transparency for law enforcement, individuals, and businesses.

For example, laws governing computer crimes grant United States law enforcement jurisdiction abroad despite geographic boundaries.[126] These laws permit United States law enforcement to "pursue not only international cases that originate or conclude in the United States, but also those cases where networks or computers in the United States are merely used as pass-throughs."[127] This broad jurisdiction could lead Congress to adopt similar language to pursue cases against United States citizens, regardless of their personal or technological location. That the same principle and definition exists in a current law should allow for seamless adaptation to the SCA.

This proposed amendment would not burden technology companies that host data centers. *Microsoft* was not about whether Microsoft could transfer the data; the issue centered on whether the SCA compelled Microsoft to do so.[128] The servers used for cloud data storage are designed to quickly transmit data around the world regardless of their location. Technology companies build these servers to make the data transfer even faster and withstand the increase in cloud computing demand.[129] Microsoft can easily

123. *See* Marketa Trimble, *Second Circuit's Decision In Microsoft v. U.S. (Data Stored in Ireland): Good News For Internet Users?*, TECH. & MKTG. LAW BLOG (Aug. 1, 2016), https://blog.ericgoldman.org/archives/2016/08/second-circuits-decision-in-microsoft-v-u-s-data-stored-in-ireland-good-news-for-internet-users-guest-blog-post.htm [https://perma.cc/6VC2-JXJK].

124. *See* S.2871, 113th Cong. § 3 (2014).

125. *See* CONGRESS.GOV, *supra* note 107 ("A court issuing a warrant pursuant to this subsection, on a motion made promptly by the service provider, shall modify or vacate such warrant if the court finds that the warrant would require the provider of an electronic communications or remote computing service to violate the laws of a foreign country.").

126. *See* Herrera-Flanigan, *supra* note 30, at 320 (including the National Information Infrastructure Protection Act, the U.S.A. Patriot Act and the Computer Fraud and Abuse Act, which amended the definition of "protected computer" to include those involved in interstate or *foreign* commerce).

127. *Id*. at 325.

128. *See* Henning, *supra* note 12.

129. *See* Markoff, *supra* note 5.

transfer its data across the globe with a keystroke when compelled to do so by a warrant or MLAT agreement.[130]

However, this amendment will inevitably cause controversy within countries from which the data seizure occurs. For example, all member states in the European Union ("EU") classify privacy as a fundamental right-the United States does not hold privacy in such a high regard.[131] The United States and the EU have already clashed on the movement of data overseas.[132] There will inevitably be another disagreement of privacy rights with this amendment's enactment. However, the amendment impacts only those who are United States citizens. The amendment gives no authority for seizure of data from other countries' citizens that may maintain different privacy expectations. Further, countries like Australia, Canada, Denmark, France, Germany, Ireland, Japan, Spain, and the United Kingdom cannot conflict with the United States over this amendment because their laws already empower them to access data stored outside their own borders.[133]

B. Second Proposed Amendment: United States Law Enforcement Has Jurisdiction Over Data Physically Stored in the United States

Congress should impose jurisdiction over data stored in data centers located in the United States.[134] This way, courts assert jurisdiction over companies because of the location of the data and, more than likely, this data is for users in the United States who may not be citizens or cannot be identified as such.[135] This improves the customer experience by assuring the quick delivery of their data.[136]

Without this amendment, electronic service providers could evade civil and criminal investigations and charge consumers a premium for their privacy

130. *See* Henning, *supra* note 12.

131. *See* Steven S. McCarty-Snead & Anne Titus Htlby, *Research Guide to European Data Protection Law*, 42 INT'L J. LEGAL INFO. 348, 350 (2014) (maintaining the fundamental privacy right through the European Convention for Human Rights and the Charter of Fundamental Rights); *see also* Domingo R. Tan, *Personal Privacy in the Information Age: Comparison of Internet Data Protection Regulations in the United States and European Union*, 21 LOY. L.A. INT'L & COMP. L. REV. 661, 671 (1999).

132. *See* Mark Scott, *In Europe-U.S. Clash on Privacy, a Longstanding Schism*, N.Y. TIMES (Oct. 7, 2015), https://www.nytimes.com/2015/10/08/technology/in-europe-us-clash-on-privacy-a-longstanding-schism.html?mtrref=www.google.com&gwh=4540E44F9CD47CA4B0CD0E2F8086A12A&gwt=pay [https://perma.cc/63LG-VFA5].

133. *See* Winston Maxwell & Christopher Wolf, *A Global Reality: Government Access to Data in the Cloud* (May 23, 2012), https://www.hldataprotection.com/uploads/file/Revised%20Government%20Access%20to%20Cloud%20Data%20Paper%20(18%20July%2012).pdf [https://perma.cc/Y5QR-Y8QD].

134. *See* Trimble, *supra* note 123. The government argued for this interpretation of the SCA in *Microsoft Corp. v. United States*. Ely, *supra* note 58.

135. *See* Trimble, *supra* note 123.

136. Companies like Microsoft store data close to the user to increase the speed at which it is delivered. *See Microsoft*, 829 F.3d at 202; Markoff, *supra* note 5.

and security.[137] This creates a massive loophole that does not exist in physical data.[138] The United States government, just like in *Microsoft*, would be unable to access data when pertinent in an attempt to prosecute for illicit activity, despite the physical location of the data, without this amendment.[139]

In the alternative, Congress could amend the SCA to mandate data localization, company servers' location in the United States, and simultaneously gain jurisdiction.[140] This leaves great power with the government so that companies cannot dictate their own policy about the cloud and consumer data.[141] Yet, a mandate like this is increasingly unfeasible in the global Internet landscape and would increase costs greatly for technology companies.[142] A proposal like this is unlikely to succeed after recent progress by the EU to fight forced data localization.[143] Further, considering the power of technology companies to lobby Congress, mandating that all servers for United States companies must be stored in the United States is impracticable.[144] The alternative, for jurisdiction to search any data servers within the United States with a warrant based on probable cause, is much more realistic.

C. Third Proposed Amendment: Law Enforcement Needs a Search Warrant and Notice Requirement for Search of Any Electronic Communications

State and federal law require a governmental entity and law enforcement to have a warrant in order to search a suspect's home.[145] Currently, the SCA provides lower privacy protections for data stored through cloud computing than the protections afforded to data on an individual's physical computer or hard drive.[146] The SCA only enforces a warrant requirement in some cases, but not in others.[147] This proposed amendment

137. *See* Henning, *supra* note 12 (discussing the potential profit in "Crim Mail", a hypothetical service that would charge customers a premium to hide their data around the globe so as to deny feasibility in government searches).

138. *See Microsoft*, 829 F.3d at 220-21.

139. *See id.* at 221.

140. *See* Trimble, *supra* note 123.

141. *Id.*

142. *See* Woods, *supra* note 64 (questioning whether the cost would actually matter for a flush company like Google).

143. *See* Cameron Kerry & Alan Charles Raul, *The Economic Case for Preserving PPD-28 and Privacy Shield*, LAWFARE (Jan. 17, 2017, 3:19 PM), https://www.lawfareblog.com/economic-case-preserving-ppd-28-and-privacy-shield [https://perma.cc/3YWM-W5EH]; *see also* Trade in Service Agreement (TiSA) Annex on [Electronic Commerce] (Sept. 16, 2013), https://wikileaks.org/tisa/document/201505_Annex-on-Electronic-Commerce/201505_Annex-on-Electronic-Commerce.pdf [https://perma.cc/H7A6-W2E7].

144. *See* Trimble, *supra* note 123.

145. *See* Ozer & Conley, *supra* note 3.

146. *See* ERIC A. FISCHER, CONG. RESEARCH SERV., R 42114, FEDERAL LAWS RELATING TO CYBERSECURITY: OVERVIEW AND DISCUSSION OF PROPOSED REVISIONS 43 (2013).

147. *See* Kerr, *supra* note 60, at 387 (discussing limits of the SCA such as warrant requirement based on timing and provider status).

ensures protection for old emails and data stored through services, like Google Drive, while the current statute fails to protect the data with a warrant on both counts.[148] The age of data is not a relevant barometer in evaluating the level of protections it should be afforded.[149] With almost 250 million Americans on the Internet, the lack of required data protections is concerning.[150] The government must have a warrant to access these users' electronic communications.[151] The Email Privacy Act and the Law Enforcement Access to Data Stored Abroad Act called for similar warrant protections for data so that a mere subpoena did not grant law enforcement access to electronically stored data because of the age of the data.[152]

Building on existing privacy protection, this amendment mandates probable cause for a warrant, ensuring that law enforcement cannot seize a United States citizen's data by requesting it from a country that does not hold privacy rights to such a high bar. Otherwise, users have no guarantee about the existence or quality of other countries' surveillance laws that govern access to data stored within that country's physical jurisdiction.[153] These laws are also subject to change depending on power shifts and developing technology and could therefore leave users with a lower standard than probable cause to protect their data from government seizure.[154]

Google discloses to users the number of subpoenas and warrants requested under the ECPA and fulfilled by Google for United States law enforcement.[155] There were 8,182 subpoena requests from law enforcement to Google from January to July of 2016.[156] The number of requested search warrants are only about half that, 4,246, for that time period.[157] Google fulfilled 76% and 85% of these requests, respectively.[158] Google notifies the user that law enforcement has requested their data unless the request is pursuant to an emergency request or a gag order.[159] Fifteen of the twenty-four companies surveyed by the Electronic Frontier Foundation always notify a

148. *Id*.

149. *Id.* at 393.

150. *See United States*, ICT DEVELOPMENT INDEX 2016, http://www.itu.int/net4/ITU-D/idi/2017/index.html [https://perma.cc/64WJ-CJ9B] (last visited Feb. 17, 2018).

151. *See* Daniel J. Solove, *Reconstructing Electronic Surveillance Law*, 72 GEO. WASH. L. REV. 1264, 1299-300 (2004).

152. *See* THOMPSON & COLE, *supra* note 9, at 9, 13-15.

153. *See* Jennifer Granick, *The Microsoft Ireland Case and the Future of Digital Privacy*, JUST SEC. (July 18, 2016, 12:46 PM), https://www.justsecurity.org/32076/Microsoft-ireland-case-future-digital-privacy/ [https://perma.cc/A2DR-EQ8T].

154. *Id*.

155. *See Transparency Report: United States*, GOOGLE, https://transparencyreport.google.com/user-data/overview?user_requests_report_period=authority:US [https://perma.cc/PTU2-BTNF] (last visited Feb. 17, 2018).

156. *Transparency Report: United States*, GOOGLE, https://perma.cc/V9SJ-T332 (last visited Dec. 13, 2016).

157. *Id*.

158. *Id*.

159. *See Transparency Report: Legal process*, GOOGLE, https://perma.cc/9SSS-24L7 (last visited Dec. 13, 2016).

user when the government submits any kind of data request.[160] These few technology companies invest in user notice because a governmental entity is not required by the SCA to always notify the subscriber or customer of the subpoena or search warrant execution.[161] Even where notification is required, law enforcement can delay fulfilling the requirement.[162] This practice is fundamentally unfair and undermines an individual's right to due process if the person is not notified or receives delayed notification through an SCA loophole. Individuals are left to trust technology companies to protect their data and fight for their rights, despite such companies' main incentive to protect their consumer base.

D. Amendment Application to Microsoft Corp. v. United States and Microsoft's Underwater Data Centers

The United States never disclosed the citizenship of the suspect in *Microsoft*.[163] Thus, this note proceeds in hypotheticals to determine the effectiveness of the above proposals. Microsoft stores customer data in the "general" area of which the customer is located, based on a customer's selected location preference.[164] If the customer is a United States citizen, the first proposed amendment would circumvent the preferred location to grant law enforcement access to search the data with a valid search warrant. None of the proposed amendments would help the investigation if the customer was not a United States citizen unless Microsoft stored his data on a United States server. This country's law enforcement does not need the power to search everyone's data, nor should they. United States citizens and businesses understand our country's laws and make a conscious choice to retain citizenship and do work here, and therefore, are subject to United States law.

The second suggested amendment provides United States courts and law enforcement jurisdiction over the underwater data centers that connect to the United States. Each data center, whether it floats in the ocean or rests on the ocean floor, must connect to the mainland to transmit the data to the company or the user.[165] Since the data center needs to link to an office and control center, the company operating the data center needs to maintain a physical presence within the geographical borders of the United States, thus giving the underwater data centers a geographic location for searches.

The third amendment does not solve the issues presented by *Microsoft* or the underwater data servers. However, it would protect customers in this

160. Who Has Your Back?, ELEC. FRONTIER FOUND., https://perma.cc/N4M6-34PU (last visited Dec. 13, 2016).

161. *See* 18 U.S.C. § 2703(b).

162. *See* Orin S. Kerr, *The Future of Internet Surveillance Law: A Symposium to Discuss Internet Surveillance, Privacy & the USA Patriot Act: Surveillance Law: Reshaping the Framework: A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1233-34 (2004).

163. *See Microsoft*, 829 F.3d at 203 (revealing the warrant only asked for the email address).

164. *Id*. at 202.

165. *See* Markoff, *supra* note 5.

constantly evolving world of technology by holding the government to a probable cause standard no matter the type or age of the data.[166] The Internet and the cloud will inevitably evolve to allow for more storage for various types of data, to the point where it will be a user's main use of electronic storage.[167] This mass of data should be protected like a physical data and should not be discriminated against because it may be easier to access.

V. CONCLUSION

The Stored Communications Act revolutionized the privacy laws of the Internet in 1986. Yet, the rapid development of the world of technology and the lack of modernization to the law curtailed its effectiveness. Judge Lynch recognized that the *Microsoft* decision was the byproduct of an ineffective statute to govern that particular set of facts. Law enforcement should not have access to all data stored around the world, but Congress needs to empower, not hamper, them in doing their jobs effectively by allowing them access to the data of United States citizens. The current Stored Communications Act does the former. Recent Congressional attempts have similarly been insufficient to amend this foundational statute. Even though the Supreme Court granted *certiorari* to hear the case, Congress must act to create a thorough legislative solution to deal with the domestic and international issues posed in *Microsoft*.

The record of *Microsoft* is silent as to the citizenship of the suspect. If he was a United States citizen, the first proposed amendment in this note would govern the proper seizure of the data based on probable cause. The underwater data centers would fall under the jurisdiction of United States jurisdictions in accordance with the first and second proposals. Whether the data is anchored to the sea floor or floating off the California coast, it is operated by a United States company and likely contains the data of United States citizens living close to the coast.

The legal landscape surrounding data, Congress, and law enforcement in this area is complicated. There are a number of players and considerations to factor in on the domestic and international levels. The proposed amendments in this note are not exhaustive in the mission to fully rectify the Stored Communications Act. There is much more to contemplate regarding differentiating data types, international ramifications, and surveying the methodologies of cloud storage companies for an impactful and nuanced solution. Congress must update the Stored Communications Act to balance the interests of users, United States citizens, international implications, and law enforcement.

166. These ideas of data distinction and age are further discussed in Kerr, *supra* note 60, at 376.

167. *See* Anderson & Rainie, *supra* note 75.