A LOCATION-BASED TEST FOR JURISDICTION OVER DATA: THE CONSEQUENCES FOR GLOBAL ONLINE PRIVACY

Shelli Gimelstein†

Abstract

U.S. technology companies face growing uncertainty over whether and how they can be compelled to turn foreign-stored user content over to law enforcement officials. In July 2016, the Second Circuit ruled that the government could not require Microsoft to produce user content stored on its server in Ireland because the execution of the government's warrant constituted an impermissible extraterritorial application of the Stored Communications Act (SCA).[1] *But after the Second Circuit declined to rehear Microsoft Corp. v. United States, (formally titled In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, also known as the "Microsoft Ireland" case) en banc in January 2017, the Supreme Court granted the DOJ's petition for certiorari and heard oral argument on the case in February 2018.*[2] *Throughout this litigation, other courts have issued orders compelling Google to produce foreign-stored data requested by SCA warrants.*[3] *Two fundamental questions have divided these courts: (1) whether the physical location of the data at the time it is accessed should determine whether it is within the reach of the SCA, and (2) whether other countries' data privacy laws and search-and-seizure protections apply.*[4]

---

† J.D. Candidate, Stanford Law School, 2018. Thank you to Jennifer Granick for supervising my work and providing invaluable guidance, and to Richard Salgado and Al Gidari for sharing your insights and expertise on this topic. I am also grateful for the helpful comments of Bernadette Meyler, Dan Ho, and the students in the Fall 2016 Stanford Legal Studies Workshop on the earliest version of this piece. An additional thank you to the staff and editors at the University of Illinois *Journal of Law, Technology & Policy* for their edits and feedback throughout the revision process.

1. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.*)*, 829 F.3d 197, 209 (2d Cir. 2016).

2. As of this writing, the Supreme Court has not yet issued a ruling in *Microsoft Ireland*, and Congress has not passed any legislation that would resolve the issues at the heart of this case.

3. *In re* Search Warrant, No. 16-960-M-01 To Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017); *see also* In The Matter Of The Search Of Content That Is Stored At Premises Controlled By Google, 2017 WL 1398279 (N.D. Cal. 2017).

4. *Microsoft Corp.*, 829 F.3d 197; *In re* Search Warrant, 232 F. Supp. 3d 708; In The Matter Of The Search Of Content That Is Stored At Premises Controlled By Google, 2017 WL 1398279.

This Article argues that basing government jurisdiction over data on the data's physical location threatens user privacy. It also creates unworkable and unpredictable results for technology companies by failing to account for the significant differences in how they divide, store, and transmit their users' data around the world. In the context of digital searches, the data location test has two potential effects. First, it will create bottlenecks in the already-burdensome mutual legal assistance system, hindering intergovernmental cooperation on law enforcement investigations. Second, it may embolden foreign governments to circumvent the system by adopting similar, or even more extreme, positions on jurisdiction over data, such as data localization and mandatory encryption backdoor laws. These policies have dangerous consequences for privacy, free expression, and innovation around the world.

While some have written about the data location test in Microsoft Ireland in the abstract,[5] *this Article takes a step further and considers its role in the rulings conflicting with Microsoft Ireland that have been issued by federal judges over the past two years.*[6] *It also evaluates several recent legislative and non-legislative proposals to solve the problems arising from the data location test. In particular, this Article highlights the pressing need for Congress to reform the Stored Communications Act, incorporating an alternative test for jurisdiction over user data and provisions that would clarify companies' data disclosure obligations under conflicting legal regimes. Finally, while much of the literature on this topic focuses solely on legislative proposals rather than the real-world impact of the uncertainty creating a need for statutory reform,*[7] *this Article focuses on what companies should do while they await a resolution from Congress or the Supreme Court. To that end, this Article offers some practical recommendations for how companies can navigate the issues arising from the data location test, particularly as they make decisions about their global operations and data storage architecture.*

TABLE OF CONTENTS

5. *See* Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST, (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case/?utm_term=.99b682ec803e (discussing the initial impacts of the Microsoft Ireland case).

6. *See, e.g.*, *In re* Search Warrant No. 16-960-M-1, No. 16-960, 2017 U.S. Dist. LEXIS 131230 (E.D. Pa. Aug. 17, 2017) (elaborating on the Microsoft/Ireland data location test); *see also In re* A Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014).

7. *See, e.g.*, Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (Apr. 2016) (discussing potential legislative solutions to the issues raised by the Microsoft Ireland case).

INTRODUCTION

Gaining access to data about a suspect's online activity is a critical component of modern law enforcement investigations.[8] However, courts have struggled to apply well-established Fourth Amendment jurisprudence on physical searches and seizures to digital data.[9] Cloud-based web services, which track users' daily locations and activities and store their most sensitive personal information, lack a defined physical location because U.S. technology companies house their data storage infrastructure all over the world.[10] This makes it difficult for courts to determine whether and how the U.S. government may access this data for law enforcement, national security, and surveillance purposes. Conflicting government interests and statutory regimes make the process of mutual legal assistance challenging and slow, impeding intergovernmental cooperation on cross-border investigations. Meanwhile, technology companies that store user data are left in an untenable position wherein they must either violate one country's laws by withholding the data its government seeks, or violate another country's laws by complying with another government's request.[11]

The Stored Communications Act (SCA), which establishes procedures to obtain electronic communications data in the U.S., illustrates the problem with relying on data's physical location for defining the boundaries of where a government has jurisdiction or where its laws apply.[12] The SCA, which is part of the Electronic Communications Privacy Act (ECPA), was passed in 1986, when Congress could not have fathomed today's global, interconnected internet infrastructure, or how difficult it would be to determine how domestic warrant procedures apply to data located in the cloud.[13] In referring to the "facility" where the data is stored or through which electronic services are provided,[14] the SCA seems to force courts to look only at where data is physically located to determine whether the U.S. government may obtain data from outside of the U.S. pursuant to the SCA. This approach to domestic digital searches has

8. *See id.* (discussing the complexity of including multiple jurisdictions when seeking cloud data).
9. *Id.* at 786.
10. *Cisco Global Cloud Index: Forecast and Methodology, 2015-2020*, CISCO (2016), http://www.cisco.com/c/dam/en/us/solutions/collateral/service-provider/global-cloud-index-gci/white-paper-c11-738085.pdf (forecasting that global cloud IP traffic will account for more than ninety-two percent of total data center traffic by 2021 and that fifty-nine percent of the internet consumer population will use personal cloud storage).
11. Woods, *supra* note 7, at 749.
12. Stored Communications Act, 18 U.S.C. §§ 2701–12 (2018).
13. Woods, *supra* note 7, at 749.
14. 18 U.S.C. § 2701(a) (2018).

consequences beyond U.S. borders.[15] As discussed below, the approach can embolden foreign governments to adopt similar—or even more extreme—positions on jurisdiction over data that will negatively impact privacy, free expression, and innovation around the world. More broadly, the debate over where SCA warrants apply reflects the difficulty of determining when governments can have access to data on the global internet. This problem is especially important to technology companies that operate in countries with differing legal standards and values surrounding online privacy, particularly if they want to avoid participating in breaches of user privacy. For this reason, companies have a major stake in the question of which laws apply to their users' data.

Part I of this Article will summarize the debate over whether government jurisdiction over data should be determined by its physical location. Informed by the scholarly critiques of the data location test, Part II discusses the Second Circuit's July 2016 ruling in *Microsoft Corp. v. United States* (formally titled *In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation*, also known as the "Microsoft Ireland" case). The Author argues that the Second Circuit's ruling in this case illustrates the problem in relying on data location as a basis for determining where SCA search warrants can lawfully be executed. The Second Circuit's ruling turns on whether user privacy is the focus of the SCA, and whether the government's violation of privacy through the execution of an SCA warrant occurred domestically or abroad. While the Second Circuit may have found a short-term answer to this question in the case of Microsoft, there may be no way to resolve this issue for other companies with different data storage architecture, such as Google. It remains to be seen whether this dilemma can be resolved by the Supreme Court or Congress.

Part III will evaluate potential legislative and non-legislative solutions to the problems the *Microsoft Ireland* ruling brings to light. Specifically, the Author argues that courts should develop an alternative test that considers factors like where the company controlling the data is located, the country where the suspect is located, the suspect's country of citizenship, or where the crime occurred. Legislators have proposed several bipartisan bills incorporating these factors into the basis for issuing warrants, but these bills have stalled in the Senate, and Congress should renew its focus on passing these bills. Part III also discusses some proposals aside from ECPA reform, such as revising and streamlining the Mutual Legal Assistance Treaty (MLAT) process and creating local data "trustees" in the countries in which companies operate. In Part IV, the Author analyzes how failing to amend the SCA and leaving *Microsoft Ireland* as good law may increase bottlenecks in the Mutual Legal Assistance process and encourage countries to circumvent U.S. legal processes through data localization laws, mandatory encryption backdoors, and other policies that harm user privacy and hinder technological innovation. These consequences highlight the pressing need to abandon the data location test for defining the scope of the

15. *See* Woods, *supra* note 7, at 778 (discussing the likelihood of the current U.S. doctrine fostering reciprocity with foreign jurisdictions).

SCA and as a basis for government jurisdiction to apply its laws in general. Part V of this Article offers some preliminary conclusions on how both small and large companies should approach the issues arising from the data location test.

I. THEORIES OF JURISDICTION OVER DATA

The structure and composition of data makes it difficult to pin down its physical location. Data is inherently borderless; an email transits through a number of jurisdictions on its way from the sender to the recipient, even if both are located in the same country.[16] Additionally, unlike other forms of property, data is uniquely mobile, divisible, and commingled with other data.[17] In *The Un-Territoriality of Data*, Jennifer Daskal explains the difficulty of tracing a digital footprint back to a particular individual, particularly since multiple users' communications are often bundled together as they transit fiber-optic networks.[18] Internet service providers (ISPs) can store it in multiple locations at once and set up their networks such that data travels through various jurisdictions even if the users engaging in communications are all within the same territory.[19] As Orin Kerr notes in *The Next Generation Communications Privacy Act*, electronic "files [can] be fragmented and the underlying data located in many places around the world" such that the files "only exist in recognizable form when they are assembled remotely."[20] This makes it difficult, if not impossible, to know the territory in which data is located—and to whose laws it is subject to—at any given point in time.

Andrew Woods argues in *Against Data Exceptionalism* that for the purposes of legal jurisdiction, data should be treated no differently than other intangible assets like stocks, debts, and intellectual property.[21] He points out that courts have devised location-based jurisdiction tests for these assets, even in instances in which users are in a different physical location from the assets in question, such as offshore bank accounts or wired money.[22] While data poses a unique challenge for territoriality determinations because of its location in the cloud, disputes can be resolved through a conflict of laws analysis, wherein the state must demonstrate that it has an interest in accessing that data that outweighs competing state interests.[23]

Woods argues that this case-by-case approach can be supplemented by signing reciprocity agreements to expedite foreign government's data requests, streamlining the Mutual Legal Assistance Treaty process, or allowing countries to directly serve warrants on companies without having to go through U.S. courts.[24]

---

16. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SEC. L. & POL'Y 473, 477 (2016).
17. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 366 (2015).
18. *Id.*
19. *Id.* at 369.
20. Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 408 (2014).
21. Woods, *supra* note 7, at 735.
22. *Id.*
23. *Id.* at 774–80.
24. *Id.* at 778–79.

Daskal takes the opposite view: given the unique properties of data, traditional, territoriality-based rules for jurisdiction should not apply to law enforcement access to data.[25] Instead, depending on the constitutional and statutory context, the location of the data, the provider, or the government agent accessing the data may all be more relevant to determining jurisdiction over data separated by an international border from the person or entity accessing it.[26] Daskal notes that the various U.S. statutes authorizing warrants for data collection all employ different languages and approaches to determining territoriality.[27] For example, foreign intelligence surveillance statutes provide greater privacy protections to U.S. persons or persons located in the U.S. than to non-U.S. persons or those outside U.S. borders.[28] Wiretap Act cases suggest that territoriality should be assessed based on either the location of the data or the location of the agent accessing it, whereas the location of property appears to control territoriality for Federal Rules of Criminal Procedure (Rule 41) warrants.[29] According to Daskal, this "highlight[s] the potential arbitrariness of data location as determinative of the rules that apply."[30]

The disagreement over whether traditional jurisdiction tests can and should extend to electronic data impacts the technology industry, which has much at stake based on which interpretation of the SCA courts choose to adopt. Microsoft argues that a state may access data only if it is located within that state's territorial jurisdiction.[31] Facebook and Google, on the other hand, have taken the position that a government cannot access their users' data unless the *companies* themselves, not their physical servers, are domiciled in that territory.[32] This issue lies at the heart of *Microsoft Ireland*, in which the Second Circuit and the Supreme Court deal with the question of whether a government "seizure" of users' email data occurs at the place where data is accessed, or the place where it is stored.[33] Some have lauded the Second Circuit's adoption of the latter view as a win for privacy rights because it limits technology companies' obligations to turn over the content of their users' communications.[34] Others have criticized the ruling as unworkable in the

25. *See* Daskal, *supra* note 16, at 365–87 (describing the characteristics of data that make it unique and explaining how the Fourth Amendment applies to data).

26. *See id.* at 334–60 (explaining the constitutional, statutory, and jurisdictional application of territoriality in law, including the understanding of territoriality in connection to Fourth Amendment doctrine and warrant jurisdiction).

27. *Id.* at 355–64.

28. *Id.* at 343–54.

29. *Id.* at 355–64.

30. *Id.* at 367.

31. *See Law Enforcement Requests Transparency Report FAQ's*, MICROSOFT, https://www.microsoft.com/about/csr/transparencyhub/lerr/ (last visited Mar. 31, 2018) (stating that Microsoft challenges some law enforcement requests based on its view that "email should receive the same treatment as physical documents or other property, where the U.S. government cannot obtain a search warrant to search and seize property located outside the U.S.").

32. Woods, *supra* note 7, at 735–36.

33. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 197, 209 (2d Cir. 2016).

34. *See* Kate Conger, *Microsoft Triumphs in Warrant Case Against U.S. Government*, TECHCRUNCH (July 14, 2016), https://techcrunch.com/2016/07/14/microsoft-wins-second-circuit-warrant/ (quoting a statement

context of companies that do not store the entirety of one user's data on the physical server closest to where his network is located, but rather store it in fragments that constantly move across its various servers located all over the world.[35]

II. THE DATA LOCATION TEST IN *MICROSOFT IRELAND*

A. The Ruling

In 2013, the DOJ served a warrant on Microsoft at its Redmond, Washington headquarters, requesting both content and non-content information about a customer under investigation for drug crimes.[36] The warrant was issued by a magistrate judge in the Southern District of New York pursuant to the Stored Communications Act (SCA).[37] Section 2702 of the SCA generally prohibits service providers from disclosing the content of user communications, such as stored emails, to any third parties except the government with proper legal process, which may include obtaining a warrant for that data from a U.S. judge.[38] Section 2703 governs the conditions under which user data may be disclosed.[39] Emails less than 180 days old may be obtained only pursuant to a warrant; emails older than 180 days may be accessed with a warrant, a subpoena, or a § 2703(d) court order.[40]

In the warrant application, the government did not specify Microsoft's Dublin data center as the place to be searched, instead referring generally to information associated with an email account "stored at premises owned, maintained, controlled, or operated by Microsoft Corporation."[41] The company has 100 datacenters worldwide that are operated by wholly-owned local subsidiaries.[42] In response, Microsoft provided only the non-content data stored

made by Microsoft's Brad Smith discussing the limits on the U.S. Government's use of search warrants globally, and discussing other companies' likely reactions).

35. *See* Marketa Trimble, *Second Circuit's Decision in Microsoft v. U.S. (Data Stored in Ireland): Good News for Internet Users?*, TECH. & MKTG. L. BLOG (Aug. 1, 2016), http://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 (explaining how data may be stored across various regions or countries, and highlighting possible legal issues that arise from jurisdictional decisions based on data location).

36. *Microsoft Corp.*, 829 F.3d at 200–04; Alex Noonan, *Microsoft v. United States: DOJ Petitions for Certiorari in Microsoft Ireland, Argues that Probable-Cause Warrants Require Service Providers to Supply Data Stored Overseas*, JOLT DIGEST (July 1, 2017), http://jolt.law.harvard.edu/digest/doj-petitions-for-certiorari-in-microsoft-ireland-argues-that-probable-cause-warrants-require-service-providers-to-supply-data-stored-overseas.

37. *See* Noonan, *supra* note 36 (describing the implications of the SCA and its effect on the *Microsoft* warrant).

38. 18 U.S.C. § 2702 (2018).

39. 18 U.S.C. § 2703 (2018).

40. 18 U.S.C. §§ 2703(a), (b)(1)(a), (d).

41. *Microsoft Corp.*, 829 F.3d (2013) (No. 14-2985), https://www.eff.org/document/search-warrant-email-stored-microsoft (warrant issued in 2013; on file with the editors of the *Journal of Law, Technology & Policy* at the University of Illinois College of Law).

42. *Id.* at appx. 109.

in the U.S., arguing that the warrant could not extend to content located on its Dublin server.[43]

After the magistrate judge rejected Microsoft's motion to vacate the order, the company appealed.[44] Microsoft acknowledged that it could access the relevant emails stored abroad from within the U.S., but argued that the search of the electronic data takes place at the physical location of the server on which it is stored.[45] Accordingly, Microsoft argued that the SCA's warrant procedures do not apply extraterritorially to Ireland and the magistrate's warrant should be vacated.[46] In its brief, Microsoft also argued that Congress intended for the U.S. to obtain data stored abroad through formal cooperative mechanisms like Mutual Legal Assistance Treaties, which allow states to help each other issue and execute legal processes for data stored abroad.[47] Microsoft pointed out that "law-enforcement seizure of [customer] documents on foreign soil, against a target it might not have been able to reach but for its ability to conscript an email provider into service," had caused "international discord" by subverting EU jurisdiction over data stored and processed within its borders.[48]

On appeal, the court applied the two-part *Morrison* test to determine whether Congress intended for the SCA to have extraterritorial reach, noting the strong presumption in case law against interpreting U.S. statutes as compelling extraterritorial acts by U.S. parties.[49] First, the court looked to the plain meaning and legislative history of the SCA's warrant provisions to see if Congress had contemplated extraterritoriality.[50] As a threshold matter, the court had to decide whether the government's SCA warrant fit the traditional definition of warrant, or was more of a "hybrid" between a warrant and a subpoena by virtue of being served by a service provider rather than by a government agent.[51] FRCP Rule 41(b)(5) restricts the geographical reach of a federal magistrate judge's warrants to the U.S.[52]

In contrast, a subpoena reaches any material, including customer content, "in its possession, custody, or control regardless of the location of that information."[53] Under the SCA, a subpoena reaches any basic, non-content subscriber and transactional information, as well as content that is more than 180 days old.[54]

---

43. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.), 829 F.3d 197, 204 (2d Cir. 2016).

44. *Id.*

45. *Id.* at 203.

46. *Id.* at 209.

47. Brief for Appellant at 11, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp), 829 F.3d 197 (2015) (No. 14-2985), https://www.eff.org/document/microsofts-reply-brief.

48. *Id.* at 14.

49. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d at 210 (applying the *Morrison* test).

50. *Id.* at 210–11.

51. *Id.* at 214.

52. *See* Fed. R. Crim. P. 41(b)(5).

53. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 472 (S.D.N.Y. 2014).

54. 18 U.S.C. § 2703(c)(2) (2018).

The government argued that an SCA warrant functions like a subpoena because the Act listed both as forms of "compelled disclosure" of records—which includes contents of user accounts.[55] However, the court rejected this argument, distinguishing the government's request from subpoenas compelling banks to disclose depositor's records stored overseas.[56] It found that the records at issue here did not belong to Microsoft—the caretaker of the data and recipient of the subpoena—but rather to individual account holders who had a protectable privacy interest in the information.[57]

The court noted that unlike a traditional warrant, a § 2703 warrant "does not authorize federal agents to *search* any premises or to *seize* any person or materials. Rather, it authorizes a federal agent to require a service provider to disclose materials in its possession."[58] However, the court found that Congress "employed the term 'warrant' in the Act to require pre-disclosure scrutiny of the requested search and seizure by a neutral third party, and thereby to afford heightened privacy protection," compared to what a subpoena would provide.[59] Accordingly, the court declined to apply the "custody or control" test, instead finding that "a warrant issued under the Act cannot be given effect as to materials stored beyond United States borders, regardless of what may be retrieved electronically from the U.S. and where the data would be reviewed."[60]

In the second part of the *Morrison* test, the court looked to the "focus" of the SCA to "determine whether the case involves a domestic application of the statute" and identifying where "the conduct relevant to the statute's focus occurred."[61] To do so, the court had to consider which "territorial events or relationships" formed the "focus" of the relevant statutory provision and determine whether the domestic contacts were secondary to the statutory "focus," rendering the provision's application to the case "extraterritorial."[62] The government argued that while § 2702 focuses on privacy as a blocking provision, the statutory focus of § 2703 is actually disclosure, which occurred at Microsoft's headquarters in the U.S. after the Irish-stored emails were already accessed.[63] However, the court concluded that privacy is the focus of the SCA as a whole, and that "the locus of the SCA's privacy protections [is] at the place of data storage."[64]

Having identified the statutory focus, the court turned to the ultimate question of whether executing the warrant was an extraterritorial act by

55. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d at 201.

56. *Id.* at 216.

57. *Id.* at 215.

58. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53, 70 (2d Cir. 2017).

59. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197 at 201.

60. *Id.* at 209.

61. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d at 55.

62. *Id.* at 61.

63. *Id.* at 67.

64. *Id.* at 56.

determining where the violation of the statutory focus—here, the invasion of privacy interests protected by the Fourth Amendment—occurs. Previously, the magistrate judge and district court had held that the place where government reviews the content is the relevant place of seizure.[65] The Second Circuit disagreed, finding that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed—here, where it is seized by Microsoft, acting as an agent of the government."[66] Accordingly, since the user content was located in—and would be seized from—the Dublin datacenter, the court held that execution of the search warrant would be conducted outside the U.S., thus making it an impermissible, extraterritorial application of the SCA.[67]

B. The Practical Consequences of the Decision

The court may well have interpreted the SCA's focus correctly; with such a fuzzy, vague test for statutory construction, either privacy or disclosure could have been intended as the true focus of the law. However, the court erred in assuming that data server location represents where the "focus" of the statute is implicated[68] without analyzing why privacy is violated at this point in the chain of events—that is, at the moment when a Microsoft employee looks at the data, rather than when disclosure occurs. The court found that because Microsoft was acting as an agent of the government, the "seizure" took place at the point of initial access in Ireland.[69] However, the court's Fourth Amendment analysis is flawed because it fails to consider two important facts. First, if the account owner is a foreign citizen located overseas, he cannot invoke Fourth Amendment rights under *United States v. Verdugo-Urquidez*, which means the court's inquiry into what constitutes a search or seizure is not relevant to whether the SCA authorizes the U.S. government to compel production of his data.[70] Second, the customer's data was in Microsoft's possession within the U.S.—that is, accessible by personnel located there—prior to the warrant being issued, which meant that Microsoft was fully capable of accessing and transferring the data from Ireland to the U.S. without a search warrant at any time.[71] This means

65. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d at 204.

66. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d at 59.

67. *Id.*

68. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 2017 U.S. App. LEXIS 1274, at *12 (2d Cir. 2017) (noting that "data subject to lightning recall has been stored somewhere, and the undisputed record here showed that the "somewhere" in this case is a datacenter firmly located on Irish soil").

69. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, No. 14-2985, 2016 U.S. App. LEXIS 12926, at *59 (2d Cir. 2016).

70. Orin Kerr, *A Different Take on the Second Circuit's Microsoft Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Aug. 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/20/a-different-take-on-the-second-circuits-microsoft-warrant-case/?utm_term=.76890f2ae014; *see also* United States v. Verdugo-Urquidez, 494 U.S. 259, 260 (1990) (finding that the Fourth Amendment does not apply to the search and seizure of property owned by a nonresident alien located in a foreign country).

71. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, No. 14-2985, 2016 U.S. App. LEXIS 12926, at *50 (2d Cir. 2016) (Droney, J., dissenting).

that the user may not have had a privacy interest in the data prior to the execution of the search warrant.

As Daskal points out, cloud-based data is intangible, divisible, and mobile, making it difficult to determine where this event occurs—a fact emphasized by the dissenting judges and inadequately addressed by the majority opinion.[72] For this reason, data's physical location should not be the determining factor of where the "focus" of the statute is violated. Rather, the court should have applied a different test to determine whether the government could compel production that would not hinge on the data's physical location.

By holding that the physical location of data is the criterion for determining territoriality for the purposes for the SCA, the Second Circuit's ruling highlights two problems that are unlikely to be resolved by the Supreme Court or through legislation. First, the data location test is impracticable for companies who store their data differently from Microsoft. While Microsoft stores all of its data in bundles on one physical server in a specific country, companies like Google, Yahoo!, and Facebook do not.[73] Google stores its data in "shards" that move from one location in Google's global network of data centers.[74] This system, designed to optimize efficiency, makes it impossible to know where one user's data is being stored at any given time, including when the government issues an order compelling its production.[75] In light of the vast variety in data storage architecture within the technology industry, a number of other companies are likely to face similar problems in complying with SCA warrants.[76]

More generally, there are several unique features of cloud-based data storage models that complicate the question of where data is located and whether it can therefore be reached by an SCA warrant, making it difficult to create a rule that could apply beyond the circumstances of *Microsoft Ireland*. First, cloud service providers may be able to choose to retrieve data from multiple locations, since multiple copies of data, "for reasons of performance, availability, back-up and redundancy . . . are likely to be stored across different 'virtual' and physical machines, sometimes in different jurisdictions."[77] Second, data may be "sharded" or "partitioned" in the cloud and thus stored as fragments across a range of machines, which may be located in—and thus accessed from—multiple

72. *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearings Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. 5 (2017) (testimony of Prof. Jennifer Daskal); *see* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326 (2015) (explaining how global telecommunications makes territoriality a meaning concept for deciding data access questions).

73. *See generally* Sean Gallagher, *The Great Disk Drive in the Sky: How Web Giants Store Big—And We Mean Big—Data*, ARS TECHNICA (Jan. 26, 2012, 8:00 PM), https://arstechnica.com/information-technology/2012/01/the-big-disk-drive-in-the-sky-how-the-giants-of-the-web-store-big-data/; Katie McKissick, *Just How Does Facebook Store Billions of Photos?*, UNIV. S.C. NEWS (Nov. 2, 2015), https://news.usc.edu/ 88075/how-does-facebook-store-billions-of-photos/.

74. *In re* Search Warrant No. 16-960-M-01, 2017 U.S. Dist. LEXIS 15232, at *33 (E.D. Pa Feb. 3, 2017).

75. *Id*.

76. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 2017 U.S. App. LEXIS 1274, at *11 (2d Cir. 2017).

77. Ian Walden, *Accessing Data in the Cloud*: *The Long Arm of the Law Enforcement Agent*, SOC. SCI. RES. NETWORK (Nov. 14, 2011), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1781067.

places.[78] Third, users may upload encrypted data to the cloud, which means service providers would need to decrypt it to make it intelligible to law enforcement, and that decryption process may not necessarily take place in the same location as the physical server on which the data was stored in encrypted form.[79] Fourth, cloud-based services make it more difficult to correctly identify the user data pertinent to a law enforcement request, as service providers must "establish a link between the data held in the cloud, the user device from which data was created, submitted to, or accessed from, the cloud service and an individual user."[80] Accordingly, even if user data subject to a law enforcement request has at least one determinable physical location at the time the warrant is issued,[81] this location is not necessarily where the events constituting the invasion of user privacy interests occur. It is far from clear if an ISP's multiple-step technical process of accessing user data occurs entirely within one territory or another.

The second problem arising from the *Microsoft Ireland* case is that it makes the MLAT process more complicated and unpredictable. The Second Circuit justifies its ruling in part based on the fact that the DOJ could use its MLAT with Ireland to obtain the data from the Irish government in lieu of seeking an SCA warrant.[82] While acknowledging that the MLAT system is cumbersome, with an average wait of about ten months to receive data requested from a foreign government, the court notes that the U.S. has signed MLATs with Ireland and all other EU member states, and asserts that going through this formal process is the best way for the U.S. to preserve principles of international comity and avoid violating other nations' sovereignty.[83]

However, the Second Circuit's emphasis on international comity is misplaced. The U.S. government would undoubtedly have a more compelling legal interest in the data than Ireland if the crime occurred in the U.S. or if the suspect is an American. Moreover, unlike individuals who knowingly store their property in Ireland to ensure it is protected by Irish law—*e.g.*, to take advantage of its tax laws—Microsoft's customers are likely unaware of its data storage architecture and have not chosen to subject their data to Irish law.[84] The record is silent on the nationality of the Microsoft user in question, but if he is a U.S. citizen, the ruling may imply that Irish data protection law controls all data stored there by Microsoft, including U.S. citizens' data—even when a customer's use of Microsoft services, including alleged criminal activity, is conducted exclusively within the U.S.[85] This result would be considerably less

78. *Id*.
79. *Id*.
80. *Id*.
81. Brief for Amici Curiae Computer and Data Science Experts in Support of Appellant Microsoft Corporation, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197 (2013) (No. 14-2985).
82. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, No. 14-2985, 2016 U.S. App. LEXIS 12926, at *62 (2d Cir. 2016).
83. *Id*.
84. *See* Winston Maxwell & Christopher Wolf, *A Global Reality: Governmental Access to Data in the Cloud*, HOGAN LOVELLS (May 23, 2012).
85. *Id*.

favorable for users, given that Ireland's laws are, in a number of ways, less protective of privacy rights than those of the U.S.[86]

Additionally, the *Microsoft Ireland* ruling raises several major issues with fulfilling MLAT requests. First, only Google's U.S.-based employees can access customer email accounts, regardless of where they are stored, which means that U.S. government would be unable to obtain Google customer data stored in Ireland through the MLAT process.[87] Second, it is unclear whether Ireland or any other foreign government would have the authority to obtain U.S. individuals' data from U.S.-based ISPs in order to fulfill a U.S. MLAT request. The answer may depend on whether that foreign government has jurisdiction over the data, as well as its own search-and-seizure and electronic communications privacy laws, which may vary widely and not provide the same privacy protections as those of the U.S. Third, MLATs may hinder, rather than help, international comity in cases where a third-party country requests access to customer data. For example, German law enforcement seeking data on an American suspect who committed a crime in Germany would have to seek the data from Irish authorities, who arguably have no compelling interest in the investigation and should not be involved in or given the opportunity to obstruct German law enforcement efforts.[88]

Since *Microsoft Ireland* was decided in July 2016, most U.S. companies have treated the Second Circuit's ruling as the law in effect everywhere.[89] However, a number of courts have issued rulings contradicting the Second Circuit's conclusion, though with differing rationales for their conclusions. In *In re* Search Warrant No. 16-960-M-01 to Google, Google argued that it did not have to produce electronically stored information to the FBI pursuant to two August 2016 SCA warrants because, under *Microsoft Ireland*, those only apply to data stored within the U.S.[90] But U.S. Magistrate Judge Thomas Rueter of the Eastern District of Pennsylvania found that the actions taken by Google that he viewed as constituting search and seizure of user data—gathering the requested data on its computers in California, copying the data in California, and sending it to U.S. law enforcement agents—occurred entirely within the U.S., so the Second Circuit's extraterritoriality analysis did not apply.[91] He also noted

86. *See id.* (concluding that in Ireland, (1) "there is comparatively limited judicial oversight of disclosure requests; a High Court judge is nominated to ascertain whether the government is complying with the law and issue a report on this to the Irish Prime Minister;" (2) "No law expressly prohibits Cloud service providers from voluntarily providing customer data in response to a government request"; (3) "There is no general requirement that a Cloud service provider must notify its customers prior to disclosing their data to the government"; and (4) "Irish law allows for disclosure requests to be made on broad national security grounds, even where not directly connected to a criminal investigation [and] Irish courts may be more permissive of government requests in the context of national security investigations . . . Once a Ministerial authorization has been provided, there appear to be few limitations on the ability of government to access the information.").

87. Orin Kerr, *The Surprising Implications of the Microsoft/Ireland Warrant Case*, WASH. POST: THE VOLOKH CONSPIRACY (Nov. 29, 2016), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2016/11/29/the-surprising-implications-of-the-microsoftireland-warrant-case.

88. *See id.* (discussing how major service providers store data in various datacenters at the same time and routinely move data around).

89. *Id.*

90. *In re* Search Warrant No. 16-960-M-01, 232 F. Supp. 3d 708, 711 (E.D. Pa. 2017).

91. *Id.* at 725.

that the seizure does not interfere with the user's possessory interest if the user himself is not aware that the data is being stored overseas,[92] which is a key point made by the dissenters in *Microsoft*.[93] Similarly, U.S. Magistrate Judge Thomas B. Smith of the Middle District of Florida issued a warrant for data stored by Yahoo! overseas because the focus of Section 2703 is compelled disclosure, and the disclosure of the data would take place in the U.S. rather than extraterritorially.[94]

On April 19, 2017, U.S. Magistrate Judge Laurel Beeler of the Northern District of California also ruled in favor of compelling disclosure of data stored abroad but unlike the other two magistrates, her decision actually touched on the jurisdictional problem created by the differences in companies' data storage practices.[95] She denied Google's motion to quash the warrant for contents stored outside the U.S. and ordered it to produce all requested content that is retrievable from the U.S., finding that "unlike *Microsoft*, where storage of information was tethered to a user's reported location . . . there is no storage decision here" that would make the location of the data relevant to this particular application of the SCA.[96] With the exception of Beeler, however, magistrate judges that have reached opposite conclusions from the Second Circuit on these issues have failed to account for variety in companies' data storage models.[97] For example, in ordering Yahoo! and Google to comply with SCA warrants in February 2017, Judge Thomas Duffin of the Eastern District of Wisconsin stated that when:

> [A] service provider is subject to the jurisdiction of the court, the court may lawfully order that service provider to disclose, consistent with the SCA, that which it can access and deliver within the United States," and that it "is immaterial where the service provider chooses to store its customers' data; what matters is the location of the service provider.[98]

However, this logic is flawed: ISPs may be located and operate in multiple countries and their methods of accessing and delivering data may differ. This, in turn, affects both the extraterritoriality analysis as well as the user privacy interests at stake in any given government request for data.[99] Therefore, the location of the ISP should not be the sole factor that determines whether the

92. *Id.* at 720.

93. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 855 F.3d 53, 61–76 (2d Cir. 2017).

94. *In re* the Search of Premises Located at [redacted]@yahoo.com, Stored at Premises Owned, Maintained, Controlled, or Operated by Yahoo, Inc., No. 6:17-mj-1238 (M.D. Fla. April 7, 2017).

95. *In re* Search of Content That is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1398279, at *4 (N.D. Cal. Apr. 25, 2017).

96. *Id.*

97. *See, e.g.*, *In re*: Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, No. 17-M-1234, 2017 WL 706307, at *3 (E.D. Wis. Feb. 21, 2017) (holding that the location of the storage data is immaterial).

98. *Id.*

99. *See* Orin Kerr, *Google Must Turn Over Foreign-Stored Emails Pursuant to a Warrant, Court Rules*, WASH. POST: THE VOLOKH CONSPIRACY (Feb. 3, 2017), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/02/03/google-must-turn-over-foreign-stored-e-mails-pursuant-to-a-warrant-court-rules/?utm_term=.d9c32a3529b7 (discussing the implications of the Second Circuit's reasoning).

government can compel it to produce user data, regardless of where that data is stored.

According to Orin Kerr, the tension between these magistrate judges' rulings and the Second Circuit's opinion suggests that the DOJ has been asking judges outside the Second Circuit to reject its ruling,[100] creating further confusion for companies about when and how the government can compel them to produce their users' data. In response to the uncertainty generated by the Second Circuit and this spate of contrary rulings, Google "has reversed its previous stance and informed the government that it will comply with new Section 2703 warrants outside the Second Circuit," according to the DOJ in its reply brief to Microsoft's opposition to its certiorari petition.[101] It is likely that smaller companies have been following Google's lead, lacking the resources and clout to adopt Microsoft and Google's approach of resisting government requests over the past several years.

In oral argument before the Supreme Court, the counsel for the DOJ noted the lower courts' disagreement with the Second Circuit and urged the Court to interpret the law in its current form rather than waiting for Congress to take legislative action.[102] The DOJ echoed the argument in its certiorari petition that the status quo has greatly harmed public safety, national security, and law enforcement, and "protects only criminals whose communications are placed out of reach of law enforcement officials because of the business decisions of private providers."[103] Additionally, the DOJ reiterated its argument that the Second Circuit panel "did not properly conduct a provision-by-provision analysis" of the SCA's focus; while Section 2701 deals with preventing access to data, Section 2703 "seeks to regulate" disclosure, as evidenced by the fact that it protects ISPs from suit if they provide information to the government under court order and requires ISPs to retain electronic communications to fulfill future government requests.[104] According to the DOJ, since Section 2703 warrants function as subpoenas and "gover[n] disclosure by a person rather than access to a place," Microsoft, as a domestic recipient of such a warrant, is obligated to produce data under its control, even if it is stored abroad.[105] During oral argument, Chief Justice John Roberts seemed to agree with this interpretation of the statutory focus, pointing out in his exchange with Microsoft's counsel that the specific names of Sections 2703 and 2702 refer to "disclosure," which takes place in the U.S.[106]

Notably, the DOJ focused on the national security harms caused by restricting law enforcement's access to data without addressing how the ruling throws a wrench into the entire MLAT system—in particular, the U.S.

100. *Id.*

101. Reply Brief for the United States on Petition for Writ of Certiorari, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 209 (2d Cir. 2016).

102. Transcript of Oral Argument at 15, Microsoft Corp. v. United States., 138 S. Ct. 356 (2018).

103. Petition for Writ of Certiorari, *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 209 (2d Cir. 2016).

104. *Id.*

105. *Id.*

106. Transcript of Oral Argument at 55, Microsoft v. United States, 138 S.Ct. 356 (2018).

government's ability to even participate in it.[107] In both briefing and oral argument, the DOJ also did not mention the legal significance of ISPs' varied data storage models, even though this was the basis on which Magistrate Judge Beeler found that Google, unlike Microsoft, stored its data in such a way that the extraterritoriality analysis of the SCA warrant was irrelevant. These are just two of the broader issues that will likely continue to cause difficulty for courts, ISPs, and law enforcement officials, regardless of the outcome in this case.

While the Court may identify the technical moment of seizure in this particular case, and definitively decide how SCA provisions should be interpreted, it cannot fix the statute's flaws or craft a rule for SCA warrants that is equally workable for all companies, not just Microsoft. Without changes to the SCA, magistrate judges may continue to issue contradictory rulings with conflicting, unpredictable rationales. As Richard Salgado, Google's Head of Law Enforcement and Information Security, testified before the House Judiciary Committee, courts "resolve individual disputes in ways that are divorced from sound policy solutions, without the robust opportunity for debate among a variety of stakeholders" without "appropriately addressing the equities of users, law enforcement agencies, service providers, and foreign sovereigns."[108] According to Jennifer Daskal, "courts are simply not in a position to adopt the kind of nuanced solution that is needed to appropriately take into account the relevant security, privacy, economic, and diplomatic interests at stake;" thus, if Congress were to wait to take action and allow the courts to resolve these issues, companies would continue to face "many more months, if not years, of uncertainty, with costs to our security and privacy in the interim."[109] For this reason, it is clear that regardless of how the Supreme Court rules in this case, a legislative solution is desperately needed.

III. PROPOSED SOLUTIONS

The Second Circuit did not apply the data location test for territoriality happily.[110] Rather, it did so out of a sense of obligation given the statutory construction of the SCA.[111] In its opinion denying rehearing *en banc*, the court notes that if it were permitted to evaluate "the totality of the relevant circumstances when assessing a statute's potential extraterritorial impact . . . ." it would be able to consider "the residency or citizenship of the client whose data is sought, the nationality and operations of the service provider, the storage practices and conditions on disclosure adopted by the provider, and other related

107. *Id.*

108. *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. 5 (2017) (testimony of Richard Salgado, Director, Law Enforcement and Information Security, Google Inc.).

109. *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearings Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. 7 (2017) (testimony of Jennifer Daskal, Assoc. Professor, Am. U. Wash.).

110. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d at 209.

111. *Id.*

factors."[112] In both the majority opinion and dissents, the Second Circuit judges highlight the urgent need to reform the "anachronistic" SCA to reflect the borderless nature of data and technology companies' current data storage and processing practices.[113] The Supreme Court also emphasized this point through questions in oral argument; Justice Ginsburg noted that "[in] 1986, no one had ever heard of clouds" and Justice Sotomayor suggested that rather than imagining how Congress would have written the statute in light of today's technologies, the Court could "leave the status quo as it is and let Congress pass a bill in this new age."[114]

If Congress were to amend the law to clarify the proper scope of SCA warrants, one option would be to apply them in the same way as subpoenas: to all data, regardless of location, over which the entity has custody or control.[115] However, this is incompatible with the Second Circuit's conclusion that SCA warrants are limited by Rule 41(b)(5) in geographic scope to the U.S.[116] It could also take the approach of other countries and look to other indicators of contacts with their territory to form the basis for jurisdiction over data.[117] For example, Brazilian and U.K. laws authorize compelled production based on whether the company does business in its jurisdiction, regardless of the target's nationality or place of residence, or where the data or the provider's place of business is located.[118]

A more nuanced approach is Andrew Woods' proposal for a conflict of laws analysis, in which courts would look at the compelling interests of the various legal regimes governing that data.[119] This approach combines and weighs a number of factors like provider location and an effects test based on the jurisdiction in which the harm occurred.[120] The Irish government may not necessarily have a stake in data merely because it is located in their territory—but it may have a stake if the crime being investigated occurred on its territory. A government's interest in data would be deemed highest when it is connected to an investigation of its own citizen for committing a local crime, and is held by a provider subject to its courts' personal jurisdiction.[121] This vastly exceeds the interests of the government that happens to have territorial jurisdiction over that data at the particular moment in time that it is requested. The advantage of

112. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corporation, 855 F. 3d 53, 61 (2d Cir. 2017).

113. *Id.* at 60, 62.

114. Transcript of Oral Argument at 6, 12, Microsoft Corp. v. United States, 138 S. Ct. 356 (2018).

115. *See In re* Grand Jury Proceedings the Bank of Nova Scotia, 740 F.2d 819, 820 (11th Cir. 1984) (finding that the Canadian bank, which was subpoenaed at its Miami office, could be compelled to produce documents held in a Bahamian branch, even though this would violate Bahamian bank secrecy laws, "contrary to the interests of our nation and outweigh the interests of the Bahamas." In *Microsoft Ireland*, unlike in *Bank of Nova Scotia*, Microsoft would not have violated Irish law if it fulfilled the court order).

116. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation, 829 F.3d 197, 208 (2d Cir. 2016).

117. Daskal, *supra* note 16, at 473.

118. *Id.*

119. Woods, *supra* note 7, at 774–79.

120. *See id.* at 774–80 (explaining when a country should be able to get access to data stored in the cloud and is subject to another country's laws).

121. *Id.* at 775–78.

Woods' case-by-case analysis is its flexibility, but lawmakers may seek to adopt a better-defined test for resolving conflicts of law, particularly since many crimes are global in nature and multiple countries may have equally strong interests in applying their privacy and data disclosure laws to the communications content in question.[122] Moreover, Woods' approach would only help in addressing potential conflicts between, for example, Irish and U.S. law; it would be less useful in cases like *Microsoft*, where there is no conflict of law, but rather U.S. law simply does not allow the extraterritorial seizure.[123]

A. Pending U.S. Legislation

Lawmakers have considered these varying approaches to jurisdiction over data in proposing reforms to ECPA's outdated warrant provisions. The Email Privacy Act (EPA),[124] which passed in the House during the 2015–2016 Congress and was reintroduced and passed in the House on February 6, 2017, eliminates the provision in the SCA that permits law enforcement officials to obtain emails without a warrant if they have been stored for longer than 180 days.[125] The Senate passed the ECPA Modernization Act of 2017 on July 24, 2017 to complement the House's EPA Bill in requiring the government to obtain a warrant to obtain private communications content stored by third-party service providers.[126] While these bills do not address the extraterritorial reach of the SCA, they remove the arbitrary distinction in privacy protections for a communication based on how long it has been in storage, expanding the scope of communications that can only be obtained pursuant to a warrant.[127]

The EPA and the ECPA Modernization Act represent significant steps forward in updating the SCA to include stronger privacy protections.[128] Passing these bills would also raise the stakes of correctly deciding the extraterritoriality issue, which Congress first attempted to address through the Law Enforcement Access to Data Stored Abroad Act (LEADS),[129] introduced in the Senate on February 12, 2015.[130] The LEADS Act proposed codifying the data location test by preventing the U.S. government from accessing communications content stored abroad unless the account holder is a U.S. person.[131] In creating this exception, the Act would preserve the general rule that the physical location of

122. Shakila Bu–Pasha, *Cross-Border Issues Under EU Data Protection Law with Regards to Personal Data Protection*, TAYLOR FRANCIS ONLINE (May 24, 2017), http://www.tandfonline.com/doi/full/10.1080/13600834.2017.1330740.

123. Woods, *supra* note 7, at 775–76.

124. Email Privacy Act, H.R. 387, 115th Cong. (2017).

125. Dustin Volz, *U.S. House Passes Bill Requiring Warrants to Search Old Emails*, REUTERS (Feb. 6, 2017, 5:25 PM), http://www.reuters.com/article/us-usa-congress-emails-idUSKBN15L2N3.

126. ECPA Modernization Act of 2017, S. 1657, 115th Cong. (2017).

127. Email Privacy Act, H.R. 387, 115th Cong. (2017).

128. *Id.*; Law Enforcement Access to Data Stored Abroad Act, S. 2871, 113th Cong. (2014).

129. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

130. *Id.*

131. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. (2015).

the stored data defines the scope of search warrants.[132] Such warrants would be vacated if a court finds it would require the ISP to violate the laws of a foreign country.[133] The LEADS Act also contains provisions for increasing the efficiency and transparency of the MLAT process.[134]

The next in the series of bills addressing extraterritorial access to data was the International Communications Privacy Act (ICPA),[135] which replaced the LEADS Act's data location test with a standard that is more in sync with how technology companies structure and store user data.[136] Even Microsoft has expressed support for ICPA, which would allow law enforcement officials to obtain electronic communications "regardless of where those communications are located," pursuant to a warrant.[137] ICPA defines the legitimacy of ECPA warrants "on the basis of the nationality and location of the customer [and] . . . arguably negates the litigation in the Second Circuit by stating that ECPA warrants apply 'regardless of where such contents may be in electronic storage or otherwise stored, held, or maintained[.]'"[138] The bill requires the government to take "reasonable steps to establish the nationality and location of the subscriber or customer whose contents are sought," and permits warrants to be issued only if the subscriber or customer is a "U.S. person, a person physically located within the United States, or a national of a foreign country that has a law enforcement cooperation agreement with the United States."[139]

One difficulty with this provision is that there is no way to verify that a user has provided the correct nationality to the provider when signing up for a service.[140] Users may mask their IP addresses when signing up for an account, or their IP addresses may not reflect their actual nationality if they sign up for a service while not located in their country of origin.[141] Some providers may not even ask for a user's nationality as a condition of registration.[142] However, the government will ultimately have other investigatory tools at its disposal to establish the user's nationality, and this solution would represent a positive step forward from the data location test in terms of determining by which nation's laws data ought to govern.[143] Additionally, by limiting the permissible extraterritorial warrant procedures to those concerning U.S. persons, the bill addresses the Second Circuit's concerns about adopting the "possession, custody, or control" test—namely, that this gives SCA warrants extraterritorial

132. Caroline Lynch, *ECPA Reform 2.0: Previewing the Debate in the 115th Congress*, LAWFARE: SURVEILLANCE (Jan. 30, 2017), https://www.lawfareblog.com/ecpa-reform-20-previewing-debate-115th-congress.

133. Law Enforcement Access to Data Stored Abroad Act, S. 512, 114th Cong. § 3 (2015).

134. *Id.* at § 4.

135. International Communications Privacy Act, S. 1671, 115th Cong. (2017).

136. *Id*.

137. Press Release, Senator Orrin Hatch, Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act (May 25, 2016), http://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act.

138. Lynch, *supra* note 132.

139. International Communications Privacy Act, *supra* note 135.

140. Daskal, *supra* note 16, at 498.

141. *Id.*

142. *Id.*

143. *Id.*

reach and violates international comity.[144] Both Jennifer Daskal and Richard Salgado have advocated for SCA warrant procedures to be modified to consider the underlying user's nationality and location in their testimony during the House and Senate's hearings on the implications of *Microsoft Ireland* during the summer of 2017.[145]

In addition to its provisions on SCA warrants, ICPA also provides baseline standards and procedural protections for access to third-party nationals' data if stored by an ISP in the U.S., codifying the Ninth Circuit's interpretation of ECPA's privacy protections as applicable to foreign citizens.[146] However, ICPA does not address certain data request scenarios, such as how the U.S. may obtain data if it is stored in a country with which it does not have a cooperation agreement, or if law enforcement officials do not know the nationality of the user whose data they seek.[147]

ICPA has now evolved into the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which was introduced on February 6, just three weeks prior to the scheduled oral argument in *Microsoft Ireland*, by Senators Orrin Hatch, Christopher Coons, Lindsey Graham, and Sheldon Whitehouse. Like ICPA, it eliminates the data location test by adding a provision to the SCA that would require companies to disclose information in their "possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[148] It enables the U.S. government to enter into executive agreements with qualified foreign governments that meet the criteria for "robust substantive and procedural protections for privacy and civil liberties," allowing them to directly serve legal process on U.S. companies for user data related to "serious crime, including terrorism."[149]

Troublingly, the bill does not impose U.S. warrant requirements on these foreign governments' requests and allows them to obtain data on users that may not be nationals of their country, so long as they are not U.S. persons or are not located in the U.S. The bill allows U.S. providers to move to quash legal process from the U.S. government within fourteen days of a request if they believe it targets a non-U.S. person and would force them to violate another country's laws; a court would apply a comity analysis to the motion, taking into account factors such as the location and nationality of the user and the nature of the user's

144. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 204 (2d Cir. 2016).

145. *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearings Before the H. Comm. on the Judiciary*, 115th Cong. § 3 (2017) (testimony of Richard Salgado); *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearings Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. § 6 (2017) (statement of Prof. Jennifer Daskal).

146. *See* Suzlon Energy Ltd. v. Microsoft Corp., 671 F.3d 726, 729 (9th Cir. 2011) (holding that ECPA prohibited the electronic communication service provider from disclosing aliens' emails).

147. International Communications Privacy Act, *supra* note 135.

148. Clarifying Lawful Overseas Use of Data (CLOUD) Act, H.R. 4943, 115th Cong. (2018).

149. *Id.*

connection to the U.S. and/or the requesting foreign government.[150] However, the bill does not provide an analogous procedure for U.S. companies to challenge foreign governments' requests for user data, nor does it require foreign governments seeking U.S.-stored data to provide notice to their targets about the request so that they may challenge it. The bill also leaves open the question of how companies should deal with requests from foreign governments that have not entered into executive agreements with the U.S.

By granting the U.S. government access to data stored by U.S. providers outside the U.S., the CLOUD Act would likely moot the key issues in the *Microsoft Ireland* case. Despite providing significant clarity to law enforcement by eliminating the data location test, the bill would raise a new set of issues regarding foreign governments' access to user data. Significant revisions to this bill—particularly with respect to its low evidentiary standards and notice requirements, as well as the lack of a mechanism for individualized judicial review of foreign government orders[151]—are necessary if it is to be viewed as mutually beneficial for law enforcement officials, technology companies, and users.

As Daskal and Salgado have argued, any legislative framework that replaces the data location test should have some sort of mechanism for resolving conflicts of law when companies are compelled to disclose data that implicates the citizens or data protection laws of another country, as well as opportunities for the U.S. and foreign governments to block disclosure in certain circumstances.[152] In a more limited and privacy-protective version of the executive agreements envisioned in the CLOUD Act, the U.S. government would be required to provide notice to a foreign government when it seeks to compel ISPs in its jurisdiction to produce data on its nationals, as well as the opportunity for that government to challenge such requests in court.[153] In the event of a dispute, a judge in the requesting country's jurisdiction would apply a comity analysis, weighing "the location of and nationality of the target, the location of the crime, the seriousness of the crime, the importance of the sought-after data to the investigation, and the possibility of accessing the data via other means."[154]

Beyond modifying the CLOUD Act's provisions, Congress could take further steps to protect user privacy by passing it in tandem with the EPA and

150. Andrew Woods, *The CLOUD Act: A Welcome Legislative Fix for Cross-Border Data Problems*, LAWFARE (Feb. 6, 2018), https://lawfareblog.com/cloud-act-welcome-legislative-fix-cross-border-data-problems.

151. Camille Fischer, *The CLOUD Act: A Dangerous Expansion of Police Snooping on Cross-Border Data*, ELECTRONIC FRONTIER FOUND. (Feb. 8, 2018), https://www.eff.org/deeplinks/2018/02/cloud-act-dangerous-expansion-police-snooping-cross-border-data#_ftn1.

152. *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearings Before the H. Comm. on the Judiciary*, 115th Cong. 3 (2017) (testimony of Richard Salgado); *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearings Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. 6 (2017) (statement of Prof. Jennifer Daskal).

153. *Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights: Hearings Before the Subcomm. on Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. § 5 (2017) (statement of Prof. Jennifer Daskal).

154. *Id.* at 6.

the ECPA Modernization Act, in order to make it clear that a warrant based on probable cause would be required in order for the U.S. or a foreign government to access data stored by U.S. providers, even if the data belongs to an individual who is not a U.S. person. Additionally, in negotiating executive agreements, the U.S. may make its waiver of SCA blocking provisions conditional on the foreign government agreeing not to require U.S. companies to store their nationals' data within their jurisdiction.

With the appropriate procedural checks, a system of agreements with foreign governments could have three important benefits. First, it would establish consistent rules for data disclosure and would function as a check on both U.S. and foreign government warrant authority.[155] It would also help clarify ISPs' disclosure obligations when U.S. and foreign laws conflict, relieving the immense uncertainty ISPs currently face when ordered to give law enforcement access to user data.[156] Finally, by enabling foreign governments to access U.S.-held data in investigations of their own citizens—particularly if the U.S. conditions these agreements on the foreign government eschewing data localization laws—this legislative framework would mitigate the risk that these governments would adopt surveillance or decryption laws out of frustration at their inability to access data in situations in which the equities would weigh in favor of its disclosure to law enforcement.[157] These risks will be discussed in further detail below in Part IV.

B. Bilateral Data Sharing Agreements

The origins of the CLOUD Act's executive agreement provisions date back to the day after the Second Circuit's ruling in favor of Microsoft, when the DOJ announced plans to enter a data-sharing agreement with the U.K. This agreement allows the U.K. government to directly serve U.S. tech companies with wiretaps and warrants to search email accounts and other communications, provided that their searches do not target U.S. residents.[158] In its legislative proposal, the DOJ cited the lengthy and inefficient MLAT process as a major obstacle to legitimate government investigations, and noted that it would submit legislation "to address the significant public safety implications of the *Microsoft* decision" in order to authorize law enforcement to obtain electronic data located abroad so as to fulfill its obligations and receive reciprocal benefits under the agreement.[159]

The draft legislation authorizes the DOJ, with the concurrence of the State Department, to enter into bilateral data-sharing agreements with countries that meet certain "substantive and procedural protections for privacy and civil

155. *Id.*

156. *Id.* at 5.

157. Jennifer Daskal, *A Microsoft Ireland Fix: Time to Act is Now!*, JUST SEC. (Apr. 14, 2017), https://www.justsecurity.org/39959/microsoft-ireland-fix-time-act-now/.

158. Letter from Peter J. Kadzik, Assistant Attorney General, to Joseph R. Biden, President of the United States Senate (July 15, 2016), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf.

159. *Id.*; *see also* Lynch, *supra* note 132 (noting that Microsoft "negates the use of ECPA warrants for data stored abroad and thus eliminates the reciprocity that is the foundation of the bilateral agreement").

liberties," such as respect for rule of law and international human rights obligations.[160] These decisions will not be subject to Senate approval, or judicial or other review.[161]

The proposal appears to provide some recourse for companies by allowing them to contest a court order under the laws of the government that issued it.[162] However, the text of the U.S.-U.K. deal is not yet public,[163] and absent specific language in the agreement to the contrary, it appears that if the U.K. serves U.S. tech companies with warrants for data stored on U.S. soil, these warrants would be subject to U.K. procedural mechanisms.[164] These are codified in the Investigatory Powers Act (IPA), a sweeping expansion of the U.K.'s surveillance program that was passed by Parliament and obtained royal assent on November 29, 2016.[165] The IPA contains provisions on when and how a court order can compel a company to produce user data, but it also authorizes broad surveillance measures such as equipment interference (government hacking) and the acquisition of communications content and metadata.[166] These measures are largely exempt from transparency requirements or judicial oversight.[167] For example, interception orders do not require judicial authorization, and government decisions to exercise IPA powers can only be judicially reviewed for failure to observe proper procedures, not for whether the decision to authorize surveillance was correct.[168] The law also contains provisions, labeled as "technical capability notices," that create "obligations relating to the removal by a relevant operator of electronic protection applied by or on behalf of that operator to any communications or data."[169] This language suggests that upon government request, ISPs would have to decrypt user data or create a backdoor through which the government can bypass encryption and access it.[170] Technical capability notices appear to be enforceable against U.S. companies, as they "may be given to persons outside the United Kingdom (and may require things to be done, or not to be done, outside the United

160. CTR. DEMOCRACY & TECH., CROSS-BORDER LAW ENFORCEMENT DEMANDS: ANALYSIS OF THE US DEPARTMENT OF JUSTICE'S PROPOSED BILL (Aug. 17, 2016), https://cdt.org/files/2016/08/DOJ-Cross-Border-Bill-Insight-FINAL2.pdf.

161. *Id*.

162. *Id*.

163. Scarlet Kim & Marilyn Fidler, *The Weak Link in a Double Act: U.S. Law Is Inadequate for Proposed Cross-Border Request Deal*, LAWFARE (July 11, 2017, 1:00 PM), https://www.lawfareblog.com/weak-link-double-act-uk-law-inadequate-proposed-cross-border-data-request-deal.

164. Jennifer Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SEC. (Feb. 8, 2016), https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity/.

165. Investigatory Powers Act 2016, c. 25 (Eng.), http://www.legislation.gov.uk/ukpga/2016/25/contents/enacted [hereinafter Investigatory Powers Act].

166. Greg Nojeim & Christine Galvagna, *UK Investigatory Powers Bill Imperils Public Safety by Undermining Data Sharing with the US*, CTR. DEMOCRACY & TECH. (Sept. 6, 2016), https://cdt.org/blog/uk-investigatory-powers-bill-imperils-public-safety-by-undermining-data-sharing-with-the-us/.

167. *See id.* (criticizing the weak judicial review standard authorized by IPA).

168. *Id*.

169. Investigatory Powers Act, *supra* note 165, at § 253(5)(c).

170. Nojeim & Galvagna, *supra* note 166 (noting one of the problematic aspects of the bill is the ability to demand that providers create backdoors for law enforcement access to communications that would otherwise be encrypted end-to-end).

Kingdom)."[171] However, the IPA does not make clear whether the U.S. draft legislation would obligate companies served with a U.K. court order for U.K. citizens' data to comply under U.S. law with the technical capability notice provisions and compelled to decrypt data as well.[172]

Since U.S. law generally supports strong warrant requirements and independent judicial authorization, some have posited that the IPA jeopardizes the U.S.-U.K. data-sharing agreement, since Congress "will look skeptically at proposals to give the British Government access to user communications content more easily."[173] But while Congress may (and should) scrutinize the U.K.'s laws, it seems unlikely that Congress would opt out of making this deal a reality merely on the basis of the IPA surveillance provisions, given that the U.K. is America's closest ally and, as a democracy, otherwise meets the aforementioned human rights and rule of law criteria.[174] The DOJ, for its part, seems unconcerned; it announced the plan in July 2016 without (or perhaps despite) concerns about the Investigatory Powers Bill, which by then had already passed through one house of Parliament and was the subject of vigorous public debate.[175] The proposal remains at a preliminary stage, as Congress has not discussed it and would have to amend U.S. law in order for it to go into effect.

If the U.S.-U.K. deal is implemented through legislation and the U.K. government begins enforcing IPA provisions unrelated to its warrant procedures for obtaining stored user communications, it would be very concerning from a pro-privacy perspective. Before finalizing the deal, the U.S. government should facilitate a dialogue between American companies and U.K. officials about how these laws would apply in specific circumstances, and potentially insist on carve-outs from specific IPA provisions where necessary to ensure customer privacy. This would also serve as a model for structuring potential bilateral agreements with other nations in the future. Otherwise, technology companies will either have to submit to the IPA's encryption backdoor requirements or devise a plan for avoiding liability for failing to do so. Both options are likely to be costly and require companies to change how they design and/or sell their products outside of the U.S.

In the best-case scenario, U.S. legislation implementing bilateral data sharing agreements would foreclose foreign governments from bulk data collection, requiring them to specify the person, account, address, or personal device that is the subject of any data request served upon a U.S. company. In the context of the U.S.-U.K. deal, this would mean that the IPA's surveillance measures and mandatory decryption provisions would not apply because they would be inconsistent with the DOJ's proposed legislation.[176] This result is preferable to the U.K.'s current legislation, which enables law enforcement to compel providers that do business in its jurisdiction to produce users'

171. Investigatory Powers Act, *supra* note 165, at § 253(8).
172. *Id.*
173. *Id.*
174. CTR. DEMOCRACY & TECH., *supra* note 160.
175. Letter from Peter J. Kadzik to Joseph R. Biden, *supra* note 158.
176. Paul Rosenzweig, *The US-UK Deal is Actually Quite Good*, LAWFARE: PRIVACY PARADOX (July 19, 2017, 8:30 AM), https://lawfareblog.com/us-uk-deal-actually-quite-good.

communications content, regardless of the location or nationality of the target.[177] In theory, data-sharing agreements could solve some of the MLAT system's inefficiencies and the U.S.-U.K. deal may incentivize other countries to reform their laws so that they qualify for data-sharing agreements with the U.S. too.[178] To further address privacy and human rights advocates' concerns, U.S. lawmakers could add oversight requirements for U.K. judges, and change the DOJ's criteria for assessing potential agreement partners based on their laws and human rights records from "factors" into requirements.

Given the lack of viable alternatives to MLATs and law enforcement's pressing need to gain access to foreign-stored data, there are good reasons to adopt the U.S.-U.K. proposal. While it does create a blueprint for future agreements with other countries that meet the basic human rights and due process requirements listed in the DOJ's proposal, implementing such an agreement will be far more difficult with countries that have minimal rules governing data protection, law enforcement and intelligence activity, such as India, Thailand, and South Africa.[179] If Congress passes the CLOUD Act, paving the way for the U.S. to reach agreements with countries like these, the terms of the agreements may look very different from those the U.S. may ultimately reach with the U.K. For example, the U.S. may choose to limit the types of data that law enforcement officials from these countries could request to access, or could impose restrictions on the situations in which the data-sharing arrangement would apply. The U.K. is just one country out of many[180] that continue to demand user data from U.S. companies, and it would be disingenuous to point to the U.S.-U.K. deal or proposals like the CLOUD Act as an adequate solution to the problems posed by cross-border data requests. Regardless of whether Congress ultimately does authorize these executive agreements, it will likely take a long time to sign agreements with a significant number of countries. In the meantime, U.S. providers will likely face substantial uncertainty over how to proceed with data requests from foreign governments that have not yet reached a data-sharing agreement with the U.S.

C. Rethinking the MLAT Process

By limiting the U.S. government's ability to use SCA warrants to access data stored abroad, the *Microsoft Ireland* ruling makes it difficult for a foreign government investigating its own citizens for a local crime to obtain their communications content stored by Microsoft in Ireland.[181] Under the MLAT

177. Daskal, *supra* note 157.

178. Jennifer Daskal and Andrew Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, LAWFARE: PRIVACY PARADOX (Aug. 1, 2016, 8:52 AM), https://www.lawfareblog.com/congress-should-embrace-dojs-cross-border-data-fix-0.

179. John Landy, *Data Storage Location: Four Things to Consider*, DATA CTR. KNOWLEDGE (May 20, 2014), http://www.datacenterknowledge.com/archives/2014/05/20/data-storage-location-four-things-consider/.

180. *See* Jesse Schoff, *Top 10 Countries Requesting User Data from Tech Companies*, TECHSPOT (June 13, 2013, 12:15 PM), https://www.techspot.com/news/52895-top-10-countries-requesting-user-data-from-tech-companies.html (listing countries that request user data from Google, Microsoft, Skype, and Twitter).

181. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 220 (2d Cir. 2016).

system, foreign governments must submit a request for the relevant data to the DOJ, which on their behalf obtains a warrant from a U.S. judge based on probable cause.[182] However, this cooperation process is quite time-consuming and labor-intensive, since foreign governments often fail to include sufficient facts to establish probable cause.[183] To streamline this process, Daskal and Woods have proposed a new framework for U.S.-based providers to respond directly to foreign government requests for stored communications content, thus bypassing the MLAT process for a limited set of cases. Under the framework, the requesting entity would have to make an adequate showing of three things to obtain the data: "(i) the requesting government has a legitimate interest in the criminal activity being investigated; (ii) the target is located outside the United States; and (iii) the target is not a U.S. person (defined to include U.S. citizens and legal permanent residents)."[184] This proposal lowers the evidentiary standard of proof for issuing a warrant. The government need only show a "strong factual basis," rather than probable cause, "to believe that a crime has been, is being or will be committed and that the information [sought] is relevant and material to the investigation of the crime."[185]

The Center for Democracy and Technology has also proposed lowering the probable cause standard for foreign government requests, but out of concern for maintaining privacy protections for non-U.S. persons, limits this carve-out to cases in which the "perpetrator, victim, and location of the crime are all in the country that was making the demand for stored content."[186] While there are legitimate concerns about the privacy implications of eliminating the probable cause requirement, the Daskal-Woods proposal presents an important incremental step towards replacing the data location test with a compelling state interests test—which is the proper way of resolving conflicts of law over data. Implementing the proposal would also alleviate some of the pressures on the government-to-government legal assistance system, as well as lay the foundation for greater trust and transparency in data-sharing systems.[187]

D. Local Data Trusts

Microsoft has begun to implement a creative way to provide greater certainty to customers regarding which country's laws apply to their stored data. In November 2015, Microsoft announced plans to build two new datacenters in Germany and establish a local data "trust," wherein the German data trustee

182. *See* Greg Nojeim, *MLAT Reform Proposal: Eliminating US Probable Cause and Judicial Review*, LAWFARE (Dec. 4, 2015, 8:52 AM), https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review ("[A] country must file a request for mutual legal assistance under an MLAT treaty or other process. The Department of Justice, Office of International Affairs works with the foreign government to amass the information necessary to make the probable cause showing in court.").

183. *Id.*

184. Jennifer Daskal & Andrew Keane Woods, *Cross-Border Data Requests: A Proposed Framework*, LAWFARE: CYBER & TECH. (Nov. 24, 2015, 8:00 AM), https://www.lawfareblog.com/cross-border-data-requests-proposed-framework.

185. Nojeim, *supra* note 182.

186. *Id.*

187. Albert Gidari, *MLAT Reform and the 80 Percent Solution*, JUST SEC. (Feb. 11, 2016), https://www.justsecurity.org/29268/mlat-reform-80-percent-solution/.

Deutsche Telekom will control and oversee all access to customer data, and Microsoft will be unable to access it unless it obtains permission from the trustee or customers, and only under the trustee's supervision.[188] This plan expressly subjects local commercial cloud computing services to German data protection law and would presumably place it beyond the reach of an SCA warrant.[189]

The advantage of this approach is that it creates predictable rules for which country's laws their data centers are subject to and the circumstances under which they must disclose user data.[190] This will make European customers feel more secure, but would not avoid the conflict of laws issue that arises when U.S. law enforcement must turn to Germany to obtain data on an American suspect that committed a crime in the U.S.[191] Some governments may balk at this type of forum shopping, and this may not be the most privacy-protective solution for users, given that U.S. law has more robust due process provisions for government access to data than Germany does.[192] However, it is ultimately a business decision similar to companies placing their offices and bank accounts in certain jurisdictions for tax purposes. Microsoft's approach may catch on if European customers feel more secure about their data when it is subject to German law, but since Microsoft only began implementing the plan in the latter half of 2016, it is still too early to tell how successful this approach will be.

IV. INTERNATIONAL CONSEQUENCES: DATA LOCALIZATION AND DECRYPTION LAWS

By placing foreign-stored content beyond the reach of U.S. law enforcement, the Second Circuit's *Microsoft Ireland* ruling has created incentives for foreign governments to pass laws requiring data localization.[193] Data localization laws take a number of different forms, but typically limit transfers of certain types of data abroad or, at their most extreme, require companies to place data servers containing their citizens' data within their

188. *Microsoft Announces Plans to Offer Cloud Services from German Datacenters*, MICROSOFT EUROPE (Nov. 11, 2015), https://news.microsoft.com/europe/2015/11/11/45283/#sm.0000duxjg1l3fd8typi1xffky2v69#UrUxE7e15Z1ZRD3o.97.

189. *Id.*

190. Leonid Bershidsky, *Microsoft's Creative Solution to Data Privacy*, BLOOMBERG (Nov. 12, 2015, 8:27 AM), https://www.bloomberg.com/view/articles/2015-11-12/microsoft-s-creative-solution-to-data-privacy.

191. Liam Tung, *Microsoft: Conflicting Data Laws Could Cost Tech Companies Billions*, ZDNET (Feb. 25, 2016), http://www.zdnet.com/article/microsoft-conflicting-data-laws-could-cost-tech-companies-billions/.

192. Maxwell & Wolf, *supra* note 84 (noting that Germany's Federal Office of Criminal Investigation "may, in some instances, conduct a search or monitor ongoing telecommunications without providing notice to the target or to other affected persons . . . [and] may apply for a court order allowing for the interception and recording of electronic communications without the knowledge of the subject of the surveillance if there is evidence that the subject committed a serious offense, the offense is 'of particular gravity in the individual case,' and other means of establishing the facts would be much more difficult." This falls below the U.S. standard of probable cause. In addition, in some cases the government may issue a computer virus "to search a Cloud provider's servers, monitor ongoing communications, or collect communication traffic data without the knowledge of the target.").

193. Jennifer Granick, *The Microsoft Ireland Case and the Future of Digital Privacy*, JUST SEC. (July 18, 2016), https://www.justsecurity.org/32076/microsoft-ireland-case-future-digital-privacy/.

territory.[194] For example, if India wants to obtain data on a Microsoft user and does not have an MLAT with Ireland, it cannot turn to the U.S. if it lacks legal authority to obtain that data. This is a fairly likely scenario given that other countries have entered into far fewer MLATs amongst themselves relative to the number of MLATs signed by the U.S.[195] On the other hand, if India forces Microsoft to place its server on Indian territory pursuant to a data localization law, its foreign law enforcement agencies will have no legal problem in obtaining it. Even if India does have an MLAT with the U.S., obtaining data stored on its own soil is much easier and faster than waiting on the U.S.'s help.[196]

Countries pass data localization laws for a number of reasons. Some EU member states have adopted such measures out of concern that their citizens' data will be intercepted and subject to surveillance if it passes through the U.S., while countries like Russia have done so to facilitate spying on their own citizens.[197] Some countries have also pushed for data localization in an effort to spur homegrown economic activity and innovation.[198] China has adopted data localization laws out of distrust of U.S. intelligence agencies,[199] as well as a desire to give Chinese companies a competitive advantage and to maintain extensive control over foreign companies, particularly in critical industries.[200] While some of these countries' laws are industry-specific and others are more broad, the common thread is restrictions on the flow of their citizens' data—whether through prohibiting its transfer outside of the country or through requiring that companies build data centers located on their soil in order to process their citizens' data.

There are a number of problems with data localization laws. First, they force ISPs to build costly data storage centers and maintain in-country copies of user data, making it far more expensive and inefficient to operate abroad.[201] Smaller companies may be unable to bear such costs and will either increase prices for their services or exit these markets, denying consumers access to innovative services.[202] Companies may avoid selling their products in countries with data localization laws—even in large countries with a huge consumer base, like China—in light of the massive regulatory burden and their inability to ensure their customer data, particularly if it is sensitive health information, will remain secure and free from government surveillance.[203]

194. *See generally* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L. J. 677 (2015) (discussing data localization laws in different countries).

195. MLAT World Map, ACCESS NOW, https://mlat.info/ (last visited Mar. 31, 2018).

196. Nigel Cory, *Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?*, INFO. TECH. & INNOVATION FOUND. (May 1, 2017), https://itif.org/publications/2017/05/01/ cross-border-data-flows-where-are-barriers-and-what-do-they-cost.

197. Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 INT'L J. OF COMM. 2221, 2227 (2016).

198. Chander & Lê, *supra* note 194.

199. Sargsyan, *supra* note 197.

200. China, *in* 2016 TOP MARKETS CLOUD COMPUTING COUNTRY CASE STUDY, INT'L TRADE ADMIN., U.S. DEP'T. OF COMMERCE, http://trade.gov/topmarkets/pdf/Cloud_Computing_China.pdf.

201. Andrew Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 752–53 (2016).

202. *Id.* at 753.

203. Interview with Kate Black, Chief Privacy Officer, 23andMe, in Mountain View, Cal. (Oct. 12, 2017).

Data localization laws also allow foreign governments to compel the production of data—including of Americans—based on a much lower standard than that of the U.S., where law enforcements must obtain a warrant issued by a neutral magistrate based on a standard of probable cause.[204] Americans' data, even when it is stored by U.S.-based ISPs, would therefore be subject to foreign laws with far fewer protections for privacy and due process. Data localization laws are also harmful to privacy on a global level, as they make it easier for governments to engage in surveillance and monitoring of their own citizens' communications.[205] On a practical level, many companies cannot comply because they do not structure their data architecture in a way that allows them to store data within one country, or to verify the citizenship of their users in order to determine which of their data is subject to a localization law.[206]

The uncertainty over enforcement jurisdiction and law enforcement access to data may also embolden countries, frustrated with the status quo mutual legal assistance process, to push for more opportunities to access user data—in particular, through mandatory encryption backdoors.[207] Laws with decryption provisions, like the U.K.'s IPA, allow governments to skip the time-consuming data request process and require companies to design a way to decrypt user data stored within its jurisdiction.[208] In July 2016, Russia also passed a surveillance law with encryption backdoor provisions; according to the Electronic Frontier Foundation, the "anti-terrorism" law requires "any online service (including social networks, email, or messaging services) that uses encrypted data . . . to permit the Federal Security Service (FSB) to access and read their services' encrypted communications, including providing any encryption keys."[209] The law also requires ISPs to retain any user data they transmit—including video, telephone calls, text messages, web traffic, and email—for six months, and permits the government to access this data without a warrant.[210]

U.S. lawmakers have also contemplated mandatory decryption provisions following Apple's refusal to decrypt the iPhone of the San Bernardino shooter for the FBI in February 2016. Had the FBI succeeded in its quest to compel Apple to write new software code to decrypt the phone, foreign governments would likely begin demanding that Apple use the same software to help unlock the phones of suspects in their own criminal investigations.[211] Ignoring this danger, Senators Diane Feinstein (D-CA) and Richard Burr (R-NC) introduced the Compliance with Court Orders Act of 2016—which would make most kinds

204. Daskal, *supra* note 17, at 391, 397.

205. Daskal, *supra* note 16, at 477.

206. Daskal & Woods, *supra* note 178.

207. Daskal, *supra* note 16, at 480; *see also* Daskal, *supra* note 157 (discussing the new agreement based on U.K. authority to access encrypted data files located in the U.S. upon request).

208. Daskal, *supra* note 157.

209. Eva Galperin and Danny O'Brien, *Russia Asks for the Impossible with Its New Surveillance Laws*, ELECTRONIC FRONTIER FOUND. (July 19, 2016), https://www.eff.org/deeplinks/2016/07/russia-asks-impossible-its-new-surveillance-laws.

210. Andy Greenberg, *The Senate's Draft Encryption Bill Is 'Ludicrous, Dangerous, Technically Illiterate'*, WIRED (Apr. 8, 2016, 11:16 AM), https://www.wired.com/2016/04/senates-draft-encryption-bill-privacy-nightmare.

211. *Id.*

of encryption illegal if they do not incorporate backdoor access—immediately after the San Bernardino incident occurred.[212] Any company that offers a product, service, or device in the US or enables others to do the same would be subject to this mandate, and would therefore have to comply with court orders to provide decrypted content.[213] While this proposal failed,[214] the possibility remains that Congress could place affirmative duties on technology companies related to encryption.

V. IMPACT ON THE TECHNOLOGY INDUSTRY & TENTATIVE CONCLUSIONS

Compared to small startups, large companies like Microsoft, Google, and Facebook have more resources at their disposal but less structural flexibility in working around law enforcement requests for data.[215] They will face hard choices about fulfilling U.S. and foreign government data requests, as well as whether to relocate their servers to comply with data localization laws or exit foreign markets that require them to do so. Some users may shift toward services with strong encryption tools, such as the encrypted messaging app Signal,[216] but most will likely remain loyal to the major U.S.-based companies, and will face the privacy consequences of their decisions.[217]

Smaller companies have also been affected by the Second Circuit's *Microsoft Ireland* ruling, albeit in different ways. Other circuit courts have not yet decided the issue of whether a company's disclosure of data to the government within the U.S., rather than its initial access to the data abroad, is the moment of "seizure."[218] As in *In re Search Warrant No. 16-960-M-01 to Google*, a magistrate judge may distinguish such cases from *Microsoft* and require companies to comply with an SCA warrant,[219] creating confusion for smaller companies about whether they would be obligated to disclose foreign-stored communications content requested through an SCA warrant.[220] This may affect companies' decisions about where to store their user data, which typically hinges on what is most efficient and cost-effective for that company based on where its users are located and what kinds of services it provides.

---

212. *Id*.

213. *Id*.

214. Dustin Volz, Mark Hosenball, and Joseph Menn, *Push for Encryption Law Falters Despite Apple Case Spotlight*, REUTERS (May 27, 2016, 6:45 AM), http://www.reuters.com/article/usa-encryption-legislation-idUSL2N18O0BM.

215. *See* Joon Ian Wong, *Here's How Often Apple, Google, and Others Handed Over Data When the US Government Asked for It*, QUARTZ (Feb. 19, 2016), https://qz.com/620423/heres-how-often-apple-google-and-others-handed-over-data-when-the-us-government-asked-for-it/ (discussing the statistics of how large tech companies handle requests).

216. Elias Groll, *Microsoft vs. The Feds: Cloud Computing Edition*, FOREIGN POL'Y (Jan. 21, 2016, 5:14 PM), http://foreignpolicy.com/2016/01/21/microsoft-vs-the-feds-cloud-computing-edition/.

217. *See, e.g.*, *Most Popular Mobile Messaging Apps in the United States as of November 2017, by Monthly Active Users (in Millions)*, STATISTA (Nov. 2017), https://www.statista.com/statistics/350461/mobile-messenger-app-usage-usa/ (illustrating that the top five messaging apps in the U.S. are owned by U.S. companies).

218. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp.), 829 F.3d 197 (2d Cir. 2016).

219. *In re* Search Warrant No. 16-960-M-01 to Google, 2017 WL 4022806 (N.D. Ala. 2017).

220. *Microsoft Corp.*, 829 F.3d at 209.

In light of this uncertainty, there are several things technology companies can do while waiting for Congress or the Supreme Court to step in. First, companies should push for Congress to finally pass ECPA reform. The CLOUD Act likely has the most momentum given its concurrent timing with the Supreme Court's *Microsoft Ireland* ruling. However, companies should approach this bill with caution. They should urge Congress to seriously consider how the bilateral data sharing agreements formed under the CLOUD Act may adversely impact user privacy, particularly outside the U.S., and to implement stronger procedural safeguards such as individualized prior judicial review, notice to the foreign governments whose nationals are the subjects of user data requests, and limitations on the types of data that law enforcement can access without meeting heightened warrant standards. Second, companies dealing with or anticipating government requests under the SCA should not assume that the Second Circuit's ruling has precedential effect. They should ask courts to clarify their stance, while challenging the order until the court specifically authorizes it. Third, companies should carefully consider how their data storage decisions may affect which laws apply to them. For example, companies that use distributive web services, like Amazon Web Services, should verify which data center hosts their data and the geographic region in which that center is located.[221] On a more general level, companies that use or plan to develop their own data storage architecture should base their decision to store data in a given country based on whether it upholds due process and the rule of law. This will help them know what to expect and to adjust accordingly. Strategically relocating abroad to escape the U.S. government's ability to compel disclosure is unlikely to shield users from privacy violations, as the government has other ways of obtaining user communications content from foreign governments even if the Second Circuit's ruling is upheld. If the government does not need to seek an SCA warrant, officials will not need to demonstrate probable cause, which sidesteps judicial review and statutory privacy protections.[222] Thus, relocating data abroad may not yield positive results for user privacy in the long run. At the same time, network efficiency and other considerations may make it necessary to store at least some user data abroad.[223] Under these circumstances, companies should verify the particular rules that govern them in the locations they operate in. They should also try to develop strong working relationships with local officials to prevent regulations on data storage and disclosure from posing onerous financial burdens and threatening user rights.

The Supreme Court's ruling will inevitably affect how U.S. government officials and companies cooperate with foreign governments on law enforcement issues in the future, as well as the laws other countries will adopt on data storage and compelled production. The Second Circuit may have wanted

221. *See AWS Global Infrastructure*, AMAZON WEB SERVS., https://aws.amazon.com/about-aws/global-infrastructure/ (last visited Mar. 31, 2018) (detailing Amazon Web Services' global presence and services deployment).

222. Karlin Lillington, *Microsoft Ireland Faces a Data Privacy Battle in the US Supreme Court*, IRISH TIMES (Nov 2, 2017, 5:55 AM), https://www.irishtimes.com/business/technology/microsoft-ireland-faces-a-data-privacy-battle-in-us-supreme-court.

223. Woods, *supra* note 7, at 752–53.

to shield companies from governmental overreach and protect user privacy, but the reasoning and outcome of its decision may yield the opposite result through its effects on foreign governments' laws and actions. However, even if the Supreme Court reaches the question of whether data location is the appropriate test, the court can only rule based on existing statutory interpretation and precedent, so it is unlikely to resolve the issue faced by companies that structure their data differently from Microsoft.[224] Regardless of how the Court rules, this makes it all the more pressing for Congress to pass legislation that explicitly replaces the data location test for SCA warrants. This new test should apply evenly to all companies regardless of how they structure their global network and data storage infrastructure. It should also account for the borderless, mobile nature of data and strike the appropriate balance between meeting the legitimate needs of law enforcement in cross-border investigations and safeguarding user privacy rights.

224. Lillington, *supra* note 222.