Fordham International Law Journal

Volume 42, *Issue* 1 *Article* 6

Rethinking the Extraterritorial Scope of the United States' Access to Data Stored by a Third Party

Sabrina A. Morris*

*

NOTE

RETHINKING THE EXTRATERRITORIAL SCOPE OF THE UNITED STATES' ACCESS TO DATA STORED BY A THIRD PARTY

Sabrina A. Morris[*]

I. INTRODUCTION

Can the United States government enforce a warrant to compel an American Internet service provider ("provider" or "ISP") to surrender a customer's data that are stored in another country? Should it be able to do so? This Note focuses on a case that was before the Supreme

* J.D. Candidate 2019, Case Western Reserve University School of Law. The author would like to thank Professor Jonathan Entin for his thoughtful comments and encouragement.

Court that addressed this question.[1] *United States v. Microsoft*, ("*Microsoft")* would have interpreted the Stored Communications Act ("SCA" or "the Act")[2] pertaining to when and how the government may compel a provider of electronic communication service to disclose customer or subscriber content information.[3] However, before the Court made a ruling, Congress passed the Clarifying Lawful Overseas Use of Data Act ("CLOUD Act") as part of an omnibus bill, which gave a legislative solution to this issue.[4] Before the CLOUD Act was passed, courts struggled to understand and apply the SCA in a technologically evolving world, where characterizing the "cloud" itself was cloudy.

The framework in which courts addressed this issue was through a territoriality lens.[5] This means that courts interpreted the application of the SCA dependent upon notions of *where* data are stored and whether US law enforcement may lawfully gain access to the data they have a warrant for if such data are stored abroad. In short, courts framed the issue as whether a provider must comply with an SCA warrant if the sought-for data are stored on a server located domestically or abroad. However, both possible answers to that issue have problematic implications, so neither would be fully satisfactory. Congressional action with regard to this issue was long overdue. Building off of the CLOUD Act, this Note proposes a version of that bill that considers the competing interests of law enforcement, users, other countries, and technology companies, rather than only physical location.

Part I of this Note provides a brief background of Fourth Amendment protections and the SCA. Part II outlines and discusses the appellate history of the *Microsoft* case. Part III analyzes the problems of both possible outcomes of the *Microsoft* issue as it was framed. Finally, Part IV discusses the most recent legislative solution to the

1. United States v. Microsoft Corp., 138 S. Ct. 1186 (2018).

2. 18 U.S.C. § 2703 (1986).

3. *Microsoft*, 138 S. Ct. at 1186. For convenience, I will refer to all internet, electronic, and cloud service providers, and other applicable providers as a "provider."

4. The Clarifying Lawful Overseas Use of Data Act was incorporated into the Consolidated Appropriations Act of 2018, Pub. L. No. 115-141 div. V, 132 Stat. 348, 1212–25 [hereinafter CLOUD Act].

5. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 476-77 (S.D.N.Y. 2014) [hereinafter *Microsoft I*]; Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 210 (2d Cir. 2016) [hereinafter *Microsoft II*].

SCA and proposes an optimal result to address cyberspace cases dealing with similar predicaments in the future.

II. FOURTH AMENDMENT CONCERNS AND THE STORED COMMUNICATIONS ACT

Standards of privacy in the United States stem from the Constitution. In particular, the Fourth Amendment protects "against unreasonable searches and seizures" by the government.[6] An established principle in Fourth Amendment jurisprudence is the distinction between government surveillance inside versus outside of one's home.[7] This distinction is based on the idea that a person does not have a "reasonable expectation of privacy" in public spaces, as opposed to the home.[8] In public, police are not required to have any "cause or order to conduct surveillance outside."[9] In private places, however, police must have a warrant issued "upon probable cause . . . particularly describing the place to be searched, and the persons or things to be seized."[10]

The inside/outside distinction helps to "ensure[] a basic balance of Fourth Amendment protection[s]" between a person's privacy and the ability of police to conduct investigations efficiently.[11] However, this distinction becomes blurred in the context of online activity that is neither clearly outside nor inside. On the one hand, online activity requires the services of a third-party intermediary, the provider.[12] Therefore, an Internet user does not have a "reasonable expectation of privacy" because the Internet is a public domain not singularly

6. U.S. CONST. amend. IV.

7. Orin S. Kerr, *Applying the Fourth Amendment to the Internet: A General Approach*, 62 STAN. L. REV. 1005, 1010 (2010).

8. *See id*. (citing Katz v. United States, 389 U.S. 347 (1967)).

9. *Id.*

10. U.S. CONST. amend. IV.

11. Kerr, *supra* note 7, at 1011.

12. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1209–10 (2004); United States v. Warshak, 631 F.3d 266, 286 (6th Cir. 2010) ("An ISP is the intermediary that makes email communication possible. Emails must pass through an ISP's servers to reach their intended recipient."). For a general definition of Internet Service Provider, see Margaret Rouse, *ISP (Internet service provider)*, TECHTARGET (Feb. 2006), https://searchwindevelopment.techtarget.com/definition/ISP [https://perma.cc/GER4-AVY2] (defining an ISP as "a company that provides . . . access to the Internet").

controlled by the user.[13] On the other hand, users do have a "reasonable expectation of privacy" online, because they have access to certain spaces on the Internet that are not accessible to the public, such as private emails, social media messaging, or other websites where a single user login is required to access an account or other information.[14]

Viewing Internet use in physical terms also blurs the inside/outside distinction. The Internet is fully contained within wires and storage devices that a police officer could not see by chance when in a public space.[15] In that sense, the Internet is inside. Users can opt for such wired connections or wireless connections.[16] If users have a wireless connection, the Internet is outside in the sense that communications are transmitted over airwaves. Airwaves can be "intercepted in the open" because they do not pass through private channels.[17] Thus, the traditional inside/outside distinction viewed purely in regards to physicality may be arbitrary depending on the type of technology a user has installed in his or her home.[18] The result is that the inside/outside distinction ceases to "capture the basic balance of Fourth Amendment protection."[19] Traditional interpretations of the Fourth Amendment were premised on the importance of physicality and location.[20] Although cyberspace has often been compared to the physical realm, the reality is that the traditional physical assumptions ingrained in the Fourth Amendment are not quite the same on the Internet.[21] There are virtually no limits on the amount of data that can

13. *See* Kerr, *supra* note 12, at 1210.

14. *Id.* at 1210–11; Zoe Argento, *Whose Social Network Account: A Trade Secret Approach to Allocating Rights*, 19 MICH. TELECOMM. & TECH. L. REV. 201, 237 (2013).

15. *Id.* at 1012.

16. Kerr, *supra* note 7, at 1012.

17. *Id.*

18. *See id.*

19. *Id.*

20. *Id.* at 1013. *See also* Alexander Dugas Battey, Jr., Note, *A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act*, 42 RUTGERS COMPUTER & TECH. L.J. 262, 267 (2016) ("[T]he possibility of electronically stored information was unforeseeable and the Fourth Amendment's protections traditionally extended only to the tangible realm. Thus, Congress enacted the Stored Communications Act in 1986 to fill that gap to apply to our 'virtual homes.'").

21. *See* Voyeur Dorm, L.C. v. City of Tampa, 265 F.3d 1232 (11th Cir. 2001) (finding city code law prohibiting adult entertainment offered to the public did not apply to company that recorded adult entertainment at a premises because the entertainment was offered only to online subscribers and not physically to the public); Kyllo v. United States, 121 U.S. 2038, 2043 (2001) ("obtaining by sense-enhancing technology any information regarding the home's interior that

be stored and accessed on a device,[22] and data can be automatically stored in any number of locations across the globe.[23] To further distance the physical world from cyberspace, users on a computer network do not necessarily have any privacy because third parties, the providers, own and operate the networks we all access and use.[24]

In light of developing technology and fear of government intrusions, Congress passed the Stored Communications Act in 1986.[25] Congress was concerned because there were no "Federal statutory standards to protect the privacy and security of [certain electronic] communications."[26] The SCA governs stored data communications and offers network account holders "Fourth Amendment–like privacy protections."[27] The meat of the SCA is contained in two sections, one

---

could not otherwise have been obtained without physical 'intrusion into a constitutionally protected area,' constitutes a search—at least where (as here) the technology in question is not in general public use") (citation omitted); Riley v. California, 134 S. Ct. 2473 (2014) (holding that officers may examine physical aspects of a cell phone but generally may not search data on a cell phone without a warrant).

22. *See* Riley, 134 S. Ct. at 2489 ("[T]he possible intrusion on privacy is not physically limited in the same way when it comes to cell phones," because they are essentially "minicomputers" with an "immense storage capacity" that are materially distinguishable from "physical realities."); Kerr, *supra* note 7, at 1013 ("Traditional Fourth Amendment rules have been crafted in light of those assumptions [physicality limits on scale and location]; the rules generally are scale- and location-specific. Those assumptions do not hold in the Internet environment. In a world of data, third-party services can always provide more data, and the data can be anywhere. No limit exists on the number, size, or location of accounts, services, or data one person can control that might contain the evidence that the government seeks.").

23. *See* Kerr, *supra* note 7, at 1013*; see also* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 202-03 (2d Cir. 2016).

24. *See* Kerr, *supra* note 12, at 1209-10 ("When we use a computer network such as the Internet, however, a user does not have a physical 'home,' nor really any private space at all. Instead, a user typically has a network account consisting of a block of computer storage that is owned by a network service provider . . . Although a user may think of that storage space as a 'virtual home,' in fact that 'home' is really just a block of ones and zeroes stored somewhere on somebody else's computer. This means that when we use the Internet, we communicate with and through that remote computer to contact other computers. Our most private information ends up being sent to private third parties and held far away on remote network servers.").

25. Stored Communications Act, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified at 18 U.S.C. §§ 2701-2712 (2012))*; see also* S. REP. NO. 99-541, at 1-2 (1986) ("When the Framers of the Constitution acted to guard against the arbitrary use of Government power to maintain surveillance over citizens, there were limited methods of intrusion into the 'houses, papers, and effects' protected by the fourth amendment. During the intervening 200 years, development of new methods of communication and devices for surveillance has expanded dramatically the opportunity for such intrusions."); Kerr, *supra* note 12, at 1208; Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 360-61 (2015).

26. S. REP. No. 99-541, at 5 (1986).

27. Kerr, *supra* note 12, at 1212.

limiting a provider's voluntary disclosures and the other setting forth when the government can compel involuntary disclosures from providers.[28] Specifically, section 2702 "generally prohibits the provider of a wire or electronic communication service to the public from knowingly divulging the contents of any communications while in electronic storage by that service to any person other than the addressee or intended recipient" with certain enumerated exceptions.[29] Section 2703 provides requirements for when the government may gain access to contents of a stored electronic communication.[30]

Whereas the "Fourth Amendment imposes *restrictions* on the government's authority to search and seize . . . , [SCA] warrants provide the government the affirmative *authorization* to do so."[31] Thus, the SCA balances individual privacy interests with the government's interest in conducting investigations. Privacy protection is exemplified by the SCA's ability to limit providers from voluntarily disclosing information about their customer communications or records.[32] It also limits the "government's ability to compel providers to disclose information in their possession about their customers and subscribers."[33]

The SCA also differentiates between content and noncontent information.[34] Noncontent information, referred to as "a record or other information pertaining to a subscriber to or customer of" a provider, is also known as "metadata" or "traffic data."[35] Such noncontent information is not the substance of the communication, but rather refers to information about the message or transmission, such as names, addresses, and length of service or transmission.[36] The SCA defines "'contents,' when used with respect to any wire, oral, or electronic communication, [as] includ[ing] any information concerning the

28. 18 U.S.C. §§ 2702-2703.
29. *Id.* § 2702; S. REP. NO. 99-541, at 37 (1986).
30. *See* 18 U.S.C. § 2703*; see also* S. REP. NO. 99-541, at 38 (1986).
31. Daskal, *supra* note 25, at 333.
32. 18 U.S.C. § 2702; Kerr, *supra* note 12, at 1213.
33. 18 U.S.C. § 2703; Kerr, *supra* note 12, at 1212.
34. 18 U.S.C. § 2703(a)-(c)
35. *Id.* § 2703(c)(1); Kerr, *supra* note 12, at 1227.
36. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473, 485 (2016); 18 U.S.C. § 2703(c)(2).

substance, purport, or meaning of that communication."[37] Content information, which has a higher standard of privacy protection, would include such information as the subject line and body of an email or the spoken message in a recording.[38] Orin Kerr, a renowned scholar in the field of cyberspace law, defined content information as "the communication that a person wishes to share or communicate with another person."[39] To analogize this in the physical world, the inside of a sealed letter would be the content information—namely the substance of the letter.[40] Similarly, any information written outside the envelope, such as names and addresses, or information surrounding the envelope's delivery would be noncontent information.[41] Congress afforded content information a higher degree of privacy "for reasons that most people find intuitive: actual contents of messages naturally implicate greater privacy concerns than information (much of it network-generated) about those communications."[42]

The SCA contains three means for a government to compel information—a subpoena, a court order, and a warrant—all of which have different requirements and outcomes.[43] SCA warrants require the highest standard of all such means to obtain disclosure under the SCA—compliance with the procedures within the Federal Rules of Criminal Procedure.[44] This high standard is required because a warrant compels the service provider to disclose everything stored in a user's account.[45] The general requirements for obtaining a warrant under the

37. *See* 18 U.S.C. § 2711(1) (stating "the terms defined in section 2510 of this title have, respectively, the definitions given such terms in that section"); 18 U.S.C. § 2510(8).

38. Kerr, *supra* note 12, at 1228; OFFICE OF LEGAL EDUC. EXEC. OFFICE FOR U.S. ATTORNEYS, SEARCHING AND SEIZING COMPUTERS AND OBTAINING ELECTRONIC EVIDENCE IN CRIMINAL INVESTIGATIONS, 122–23 (2009).

39. Kerr, *supra* note 12, at 1228.

40. *But see* Russell Hsiao, *Implications for the Future of Global Data Security and Privacy: The Territorial Application of the Stored Communications Act and the Microsoft Case*, 24 CATH. U. J.L. & TECH. 215, 242 (2015) (concluding emails "are fundamentally different from letters" because packet switching technology, which is disassembling an email and reassembling it upon receipt, "would be roughly analogous to unsealing the letter, and sending the letter and envelope separately, and hav[ing] it reassembled when it reaches its recipient").

41. *See* Kerr, *supra* note 7, at 1019.

42. Kerr, *supra* note 12, at 1228. For Kerr's in-depth analysis of why noncontent information does not require higher privacy protections equivalent to content information, see *id.* at 1228 n.142.

43. 18 U.S.C. § 2703; Daskal, *supra* note 25, at 361.

44. 18 U.S.C. § 2703(a)-(c).

45. Kerr, *supra* note 12, at 1223.

Federal Rules of Criminal Procedure require "probable cause" and an issuance of the warrant by a magistrate judge for a government search and seizure.[46] This "probable cause" standard positions the U.S. as having one of the "more robust" standards of proof compared to other nations.[47] With these considerations in mind, this Note focuses solely on SCA warrants because of their high standard and wide scope of disclosure. SCA warrants would presumably set the standard for other extraterritorial applications of the SCA.

III. CURRENT APPLICATIONS OF THE SCA REGARDING EXTRATERRITORIALITY

Microsoft was a case of first instance in the Supreme Court on the issue of whether the US government could use an SCA warrant to compel a provider to disclose data that are stored abroad.[48] The district court in *Microsoft* was the first case to hear this specific issue.[49] Following both *Microsoft*'s district court and appellate court decisions on this issue, other courts have consistently ruled in favor of the government and enforced SCA warrants for data stored abroad.[50]

The case involves Microsoft Corporation, a provider that owns and operates a web-based email service where account holders can

46. FED. R. CRIM. P. 41(d)(1)

47. *See* Daskal, *supra* note 36, at 482-83 (comparing warrant requirements of the U.S. and other countries and concluding "[t]he U.S. warrant requirement is unique . . . and more robust than what is required in most other nations").

48. *See* United States v. Microsoft Corp., 138 S. Ct. 1186, 1186 (2018)

49. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014).

50. Only a handful of courts have considered the issue and discussed the appellate court's holding in *Microsoft*. These courts have criticized the holding and have declined to follow it, instead consistently ruling in favor of the government. *See e.g.*, *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E.D. Pa. 2017) (holding SCA warrants did not violate the presumption against extraterritoriality and were enforceable abroad); *In re* Search Warrant to Google, Inc., Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017); *In re* Info. Associated with One Yahoo Email Address that is Stored at Premises Controlled by Yahoo, Case Nos. 17-M-1234 & 17-M-1235, 2017 WL 706307 (E.D. Wis. Feb. 21, 2017); *In re* Info. Associated with [Redacted]@gmail.com, Case No. 16-mj-757 (GMH), 2017 U.S. Dist. LEXIS 92601 (D.D.C. June 2, 2017); *In re* Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, 268 F. Supp. 3d 1060 (C.D. Cal. 2017); In the Matter of Search of Content that Is Stored at Premises Controlled by Google, Case No. 16-mc-80263-LB, 2017 WL 1487625 (N.D. Cal. Apr. 19, 2017); *In re* Two Email Accounts at Google, Inc., Case No. 17-M-1235, 2017 WL 2838156 (E.D. Wis. June 30, 2017); *In re* Search Warrant Issued to Google, Inc., 264 F. Supp. 3d 1268 (N.D. Ala. 2017); In the Matter of the Search of: Contents & Records Relating to the Google Accounts, 18-mc-00020, 2018 WL 942301 (S.D. Ohio Feb. 15, 2018).

send, receive, and store email messages.[51] Microsoft stores these email messages in datacenters, which have various locations both within the United States and abroad.[52] In order to increase network speed for users and reduce "network latency," or slow Internet speeds, Microsoft's system makes efforts to assign each account to the closest datacenter to the user as possible.[53] Originally, Microsoft managed where account information was stored according to the country code with which a user registered his or her account.[54] This was an automatic process.[55] Once an account was migrated, or moved, abroad, "all content and most noncontent *information* associated with the account [was] deleted from servers in the United States."[56] However, following the Second Circuit's decision, Microsoft changed its policy so that it "now automatically detects customers' *actual* location and stores their emails in datacenters nearby."[57]

In 2013, the United States District Court for the Southern District of New York ("the district court") upheld an SCA warrant "authoriz[ing] the search and seizure of information associated with a specified web-based e-mail account that is 'stored at premises owned, maintained, controlled, or operated by Microsoft.'"[58] The warrant compelled Microsoft to disclose both content and noncontent information about the account.[59] Microsoft determined that the warrant targeted an account that was hosted in its Dublin, Ireland server, with some noncontent information stored in US servers.[60] Microsoft complied with the warrant insofar as producing the noncontent information that was stored domestically, but refused to turn over the content information stored in Ireland.[61] This refusal was accompanied

51. Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 202 (2d Cir. 2016).

52. *Id.*

53. *Id.*

54. *Id.* at 203.

55. *Id.*

56. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014) (emphasis added).

57. Brief for Respondent at 57, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2) (citing *Delivering a faster and more responsive Outlook.com*, MICROSOFT (Oct. 27, 2017), https://blogs.office.com/en-us/2017/10/27/delivering-a-faster-and-more-responsive-outlook-com/ [https://perma.cc/MZ8Y-JT7P]).

58. *Microsoft I*, 15 F. Supp. 3d, at 467-68.

59. *See id.* at 468.

60. *Id.*

61. *Id.*

by a motion to quash the warrant to the extent that it directed Microsoft to produce information stored abroad.[62]

The procedural history of this case exemplifies the different stances that courts have taken when faced with extraterritoriality issues involving SCA warrants. Extraterritoriality with regard to the reach of the SCA is problematic because the United States has recognized a presumption against extraterritoriality.[63] This presumption means that "when a statute gives no clear indication of an extraterritorial application, it has none, and reflect[s] the presumption that United States law governs domestically but does not rule the world."[64]

The district court held that the SCA warrant was valid and did not violate the presumption against extraterritoriality.[65] The court reasoned that the "concerns that animate the presumption against extraterritoriality are simply not present here" because "an SCA warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored."[66] The court found the language of section 2703(a) ambiguous in its reference to the Federal Rules of Criminal Procedure, and, therefore, found guidance in the legislative history and congressional intent.[67] The court ultimately found that an SCA warrant is a "hybrid" of "part search warrant and part subpoena" because, although the process to obtain it is "like a search warrant," an SCA warrant "is executed like a subpoena in that it is served on the [provider] in possession of the information and does not involve government agents entering the premises of the [provider] to" conduct its search and seizure.[68] Additionally, the court stated other practical reasons to support its conclusion, such as the substantial burden on the government to conduct investigations due to the lack of a requirement for the provider to verify information as well as the inconvenience and inefficiency of

62. *Id.*

63. *Id.* at 475.

64. *Id.* (quoting Morrison v. National Australia Bank Ltd., 561 U.S. 247, 255 (2010) and Microsoft Corp. v. AT&T Corp., 550 U.S. 437, 454 (2007)).

65. *Id.* at 477.

66. *Id.*

67. *Id.* at 470-71.

68. *Id.* at 471.

pursing an alternative diplomatic means called Mutual Legal Assistance Treaties ("MLAT ").[69]

The United States Court of Appeals for the Second Circuit reversed the district court, holding that the SCA warrant *did* violate the presumption against extraterritoriality, so Microsoft would not have to turn over its customer's content stored abroad.[70] The Second Circuit reasoned that if "Congress intends a law to apply extraterritorially, it gives an 'affirmative indication' of that intent," whereas Congress gave no such express indication in the SCA.[71] Indeed, the Second Circuit emphasized that it is a *presumption* against extraterritoriality, and whether or not Congress intended to *limit* the statute to only domestic application is irrelevant without some explicit agreement to its application abroad.[72] The court found further guidance in the statute's language and its use of the term of art "warrant," which "is traditionally moored to privacy concepts applied within the territory of the United States."[73] The use of the term "warrant" was significant and purposeful, as was the use of other terms in the SCA, such as "subpoena."[74] There is no subpoena-warrant hybrid as the lower court found, but rather an intentional use of each word.[75] Finally, the court also noted the legislative history and its focus on privacy protection as well as its silence as to the citizenship and location of a person.[76] In a practical sense, Microsoft would have to interact with the Dublin datacenter and this could threaten values of state sovereignty and autonomy, which are already provided for through an albeit slow, but recognized MLAT process.[77]

In 2017, the Supreme Court granted certiorari to hear the *Microsoft* case.[78] However, the case became moot in April 2018 because Congress enacted, and the President signed into law, the

69. *Id.* at 474. *See* discussion *infra* Part IV.B.

70. Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2016).

71. *Id.* at 211 (citing Morrison v. National Australia Bank Ltd., 561 U.S. 247, 265 (2010)).

72. *See id*.

73. *Id.* at 212.

74. *See id.* at 212–14.

75. *Id.* at 214.

76. *Id.* at 219–20.

77. *Id.* at 220–21.

78. *See generally* United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (order granting certiorari).

CLOUD Act, which amended the SCA to address the extraterritoriality issue.[79]

IV. PROBLEMATIC EFFECTS OF AN EXTRATERRITORIAL FRAMEWORK

Before addressing the amending CLOUD Act, it is important to first understand the SCA itself and what effects could result from applying it in favor of enforcing or not enforcing the SCA warrant extraterritorially. *Microsoft* is just one example of how difficult it is to apply the SCA to modern, global providers. Ultimately, neither outcome of the lower *Microsoft* decisions is particularly satisfactory because of the blanket applications and resulting shortcomings of each approach. Microsoft itself even acknowledges that "*either* interpretation will inevitably yield some gap in coverage in the digital era."[80]

A. Consequences if the government may obtain data stored abroad via the SCA

One outcome of an extraterritorial framework provides that the government may compel US providers to disclose electronic communications within the providers' control that are stored abroad. Such a scenario would result in three main problems. First, complying with an SCA warrant may lead to a violation of a foreign country's law. Second, there would be heightened fears of US privacy intrusion abroad resulting in economic burdens for providers. Finally, foreign countries may enact data localization measures, which would shift business from the U.S. to foreign data storage companies.

One of the largest concerns about allowing the government access to data stored abroad via an SCA warrant is the international effect. Different providers utilize different technology when it comes to storing their users' data. For example,

> Google user data—such as an email, or an e-mail attachment—is not stored as one single, cohesive digital file; instead, Google stores individual data files in multiple data "shards," each separate shard being stored in separate locations around the world. And,

79. *Id.* at 1187-88.

80. Brief for Respondent at 32, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2) (advocating for Congress to legislate but insisting that, until then, the Court must stick to the SCA as it is currently written).

> Google cannot even determine where its separate data shards are stored around the world at any given time; and, even if one shard were to stay in one place, without *all* of the shards being collected and put together at once to form the actual digital file, each shard alone is a useless piece of coded gibberish. Of course, each shard might move instantaneously to somewhere else; and then to somewhere else; and so on, and so forth.[81]

Therefore, certain technology may make "it uncertain which foreign country's sovereignty would be implicated."[82] Even if a specific country is implicated, as Ireland is in the *Microsoft* case[83], there are potential conflict of laws issues that arise. *Microsoft* "presents a potential conflict of law between the United States and the European Union."[84] Refusing to comply with an SCA warrant "could lead to a contempt of court charge" in the United States.[85] Meanwhile, unilaterally seizing data of an EU citizen without first obtaining consent of Ireland, or the country involved, would violate EU data protection laws.[86]

Jennifer Daskal, a scholar who specializes in cyberspace law, noted that a complicating fact is that the SCA itself is a blocking statute,[87] which "prohibit[s] providers that do business in their jurisdiction from responding to foreign-based requests for such data, and instead require[s] the exercise of formal government-to-government requests for data."[88] The SCA consequently prohibits US-based providers from responding to properly executed foreign government requests for the content of stored communications even if

---

81. *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 724 (E.D. Pa. 2017).

82. *Id.* at 723.

83. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 15 F. Supp. 3d 466, 467 (S.D.N.Y. 2014).

84. Battey, *supra* note 20, at 282. *But see* Reply Brief for the United States at 20–22, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2) (arguing that Microsoft complied with SCA warrants seeking data stored abroad in the past without incident and SCA warrants do "not violate any individual nation's laws").

85. Battey, *supra* note 20, at 282.

86. *Id.* at 286 (concluding an SCA warrant would violate the E.U. Data Protection Directive).

87. 18 U.S.C. § 2702(a)-(b) (2018) prohibits the voluntary disclosure of electronic communications "to any governmental entity" with certain exceptions. However, a "governmental entity is defined in 18 U.S.C. § 2711(4) as "a department or agency of the United States or any State or political subdivision thereof." *See* Daskal, *supra* note 36, at 491 n.62.

88. Daskal, *supra* note 36, at 490.

a foreign government "is seeking the data of one of its own citizens in connection with the investigation of a local crime."[89] Daskal also noted that a government win "would set a dangerous precedent, allowing governments to reach data across borders without regard to the sovereign interests of other states . . . [consequently] threaten[ing] privacy on a global scale."[90] Therefore, even if no current laws would be violated, a government win could be a model for other countries to enact similar laws.[91] If that were the case, a US-based provider would be prohibited from disclosing information under the SCA's current blocking provisions, while simultaneously violating a foreign country's laws modeled after the SCA.[92] Such a seizure disregards efforts for international police cooperation and, instead, positions US control and regulation of data stored abroad above another country's interest in maintaining control over such data within its own borders.[93]

The United States argued that enforcement of the SCA warrant in the *Microsoft* case would still respect its international obligations, citing the Budapest Convention and arguments specifically directed at Ireland.[94] The validity and gravity of these international concerns is not yet clear. However, the probability of a negative international reaction appears imminent, at least to some degree.

A second problem is, following Edward Snowden's whistleblowing of widespread government surveillance, there will be heightened fears of U.S. privacy intrusion if the government can enforce SCA warrants for data stored abroad.[95] As previously noted, allowing such enforcement abroad could "establish a dangerous

89. *Id.* at 491.

90. Jennifer Daskal, *There's No Good Decision in the Next Big Privacy Case*, N.Y. TIMES (Oct. 18, 2017), https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacy-court.html.

91. *See* Jennifer Daskal, *Symposium: Justices Can, and Should, Write Nuanced Ruling to Balance Competing Interests*, SCOTUSBLOG (Feb. 7, 2018), http://www.scotusblog.com/2018/02/symposium-justices-can-write-nuanced-ruling-balance-competing-interests/ [https://perma.cc/LX9B-W8S2].

92. *Id.*

93. *See* Daskal, *supra* note 25, at 379.

94. *See* Brief for Petitioner at 46–52, United States v. Microsoft Corp., 138 S. Ct. 1186 (2017) (No. 17-2).

95. Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens the United States' Cloud Storage Industry*, 9 BROOK. J. CORP. FIN. & COM. L. 661, 663 (2015); Brief for Respondent at 57–58, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2); David S. Kris, *Trends and Predictions in Foreign Intelligence Surveillance: The FAA and Beyond*, 8 J. NAT'L SECURITY L. & POL'Y 377, 383 (2016).

precedent under which nations can unilaterally—without agreed-upon substantive or procedural standards—compel the production of data located anywhere in the world simply by asserting jurisdiction over the company controlling the data."[96] This precedent also would "arguably justif[y] any country in the world with jurisdiction over any provider (including US-based providers) from compelling, according to their own standards, access to sought-after data."[97] However, Microsoft pointed out an ironic result from a government win. Since the government's theory in *Microsoft* is that the focus of the SCA is disclosure, as opposed to storage, "[i]t would leave U.S. citizens' U.S.-stored communications unprotected, so long as they were *disclosed* overseas."[98] It could also "facilitate corporate espionage" by allowing foreign countries "to obtain proprietary business information stored" abroad.[99]

Ultimately, the United States would be announcing that its law enforcement power reaches across the globe so that it can access data stored abroad so long as it is held by a US-based provider.[100] The effects of this law enforcement power would lead to "heighten[ed] fears of U.S. privacy intrusion both at home and [abroad]."[101] Such fears would burden American providers "to interpret unclear and dated congressional legislation and attempt to construct a coherent and precise compliance policy for their business to assure certain privacy protections to their customers without violating domestic or international law."[102] Consequently, American providers would suffer from lost revenue due to fears of privacy intrusion.[103]

---

96. Daskal, *supra* note 25, at 397.

97. Daskal, *supra* note 36, at 490.

98. Brief for Respondent at 12, 21, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2) (emphasis added).

99. Andrew Pincus, *Why is the U.S. government trying to help Vladimir Putin access information stored in the United States?*, SCOTUSBLOG (Feb. 9, 2018, 2:05 PM), http://www.scotusblog.com/2018/02/symposium-u-s-government-trying-help-vladimir-putin-access-information-stored-united-states/ [https://perma.cc/JRL9-MNNV].

100. Although the US government's power still has constitutional constraints, its authority would be expanded if the government could bypass the MLAT process and obtain data stored abroad via SCA warrants without any input of foreign nations. *See* Schultheis, *supra* note 95, at 691.

101. *Id.* at 663.

102. *Id.*

103. *Id.* at 663–64.

In fact, providers have already begun to feel the negative economic effects. For example, in the wake of Snowden's whistleblowing, the German government ended its contract with Verizon, and the Brazilian government announced it would not renew its license agreement with Microsoft.[104] Also, original reports estimated that cloud computing providers could lose anywhere from US$22 billion[105] to as much as US$180 billion in revenue in the years following the Snowden revelations.[106] However, a more recent Forrester survey revealed that losses may only amount to US$47 billion for the period from 2014 to 2016, which was lower than initially predicted, but still significant.[107] Microsoft contended that the multibillion-dollar US cloud computing industry is built on the trust of its customers, and a government win would eliminate that trust, seriously damaging those providers.[108]

Foreign governments may also react to a government win in the *Microsoft* case by enacting data localization laws that would likely be directed towards those nations' own citizens.[109] Such laws would require nationals to "store [their] data with locally-based providers so as to ensure that the data [are] subject [only] to that nation's jurisdiction."[110] Data localization efforts operate when an individual or government removes their business from US providers to local ISPs because that may be the only safeguard against actual or perceived US intrusion into data stored abroad, even if the account holder of such data is a non-US citizen living abroad.[111] Russia, for example, already enacted a data localization measure in 2015, which "requir[es] Internet

104. Battey, *supra* note 20, at 287.

105. Daniel Castro, *How Much Will PRISM Cost the U.S. Cloud Computing Industry?*, The INFO. TECH. & INNOVATION FOUND. (Aug. 2013), http://www2.itif.org/2013-cloud-computing-costs.pdf?_ga=2.92692253.1254667291.1515781499-1904554765.1515781499 [https://perma.cc/J6VK-9CM7].

106. Claire Cain Miller, *Revelations of N.S.A. Spying Cost U.S. Tech Companies*, N.Y. TIMES (Mar. 21, 2014), https://www.nytimes.com/2014/03/22/business/fallout-from-snowden-hurting-bottom-line-of-tech-companies.html.

107. Ed Ferrara, *Government Spying Will Cost U.S. Vendors Fewer Billions Than Initial Estimates*, FORRESTER (Apr. 1, 2015), https://www.forrester.com/report/Government+Spying+Will+Cost+US+Vendors+Fewer+Billions+Than+Initial+Estimates/-/E-RES122149 [https://perma.cc/73BH-HQLE].

108. Brief for Respondent at 57–58, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2).

109. *See* Daskal, *supra* note 25, at 392.

110. *Id.*

111. *See* Battey, *supra* note 20, at 287.

companies to locate their computer servers that contain personal information on Russian citizens within [Russia's] borders."[112] Additionally, "allowing governments to reach data across borders without regard to the sovereign interests of other states" would "threaten privacy on a global scale."[113] Other governments may follow the United States' example and "[assert] the same authority," conceivably even as retribution.[114]

Whether or not law enforcement's access to data stored abroad would be an intrusion, such data localization laws would, nevertheless, act as a nation's assertion of sovereignty.[115] A government win could lay the foundation for these laws simply due to tension.[116] This fear may or may not be justified. Still, fear will simply lead to global isolation, at least with regard to Internet services, handicapping providers from growing and users from getting competitive online services.[117] Although a government win would seem to aid in law enforcement efforts to conduct investigations that transcend U.S. borders, an ironic consequence may actually ensue.[118] If data localization movements succeed, law enforcement's access to extraterritorial data will actually be compromised if data ends up in the hands of foreign providers.[119] Data localization laws may also, however, develop as a response to a Microsoft win, as will be discussed in the following section.[120]

The foregoing concerns highlight the potentially unappealing outcomes of interpreting SCA warrants as allowing the government to obtain content data that are stored outside US borders. These concerns are neither completely comprehensive nor actually imminent, as there may be other consequences not yet taken into account or they may be mitigated or simply not materialize as predicted. Nevertheless, they would have appeared to present a strong possibility of occurring.

---

112. Hsiao, *supra* note 40, at 219.

113. Daskal, *supra* note 90.

114. *Id.*

115. *See* Daskal, *supra* note 36, at 476–78; Brief of Members of Congress as Amici Curiae Supporting Respondent at 21, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2); Schultheis, *supra* note 95, at 663 ("[D]ata localization movements [may be enacted] in the hopes of sheltering customers from the expansive jurisdictional reach of the SCA warrant.").

116. Hsiao, *supra* note 40, at 218–19.

117. *See* Daskal, *supra* note 36, at 478; Brief of Members of Congress as Amici Curiae Supporting Respondent at 22, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2).

118. *See* Daskal, *supra* note 25, at 393.

119. *Id.*

120. *See infra* Part IV.B.

B. Consequences if the government may not compel ISPs to disclose data stored abroad

The other outcome of an extraterritorial framework provides that the government may *not* compel US service providers to disclose electronic communications within the providers' control that are stored outside the borders of the United States. This circumstance would produce its own set of problems. First, whether an SCA warrant may compel stored data abroad could be somewhat arbitrary, depending on a provider's business decision about where to store data. Second, it would burden law enforcement. And lastly, it may also fuel a kind of data localization movement.

One of the more disturbing effects of a Microsoft win would result in a troubling dependence upon happenstance. As Daskal aptly puts it, unlike tangible property,

> we delegate large quantities of our digital property to the control of others. Vast quantities of electronic data are now held, or otherwise controlled, by third parties, including ISPs, cloud service providers, and companies that maintain and operate the fiber-optic cables that make up the Internet's backbone. Moreover, it is the third party, not the user, that generally makes the critical decisions about the path by which data travels or where it is stored. It is also the third party, not the user, that is often called on by government officials to collect and produce the sought-after data.[121]

Users generally cannot dictate where or how their data are stored or moved.[122] Rather, the third-party provider controls the data to execute its own business decisions.[123] Such decisions may promote, for

121. Daskal, *supra* note 25, at 377.
122. *Id.* at 378.
123. *Id.* at 377.

instance, obtaining efficient Internet speeds and reducing network latency,[124] or they may aim for "the most cost-effective" solution.[125]

Reliance on the location of data gives a provider immense power by allowing it to circumvent law enforcement's access to certain data.[126] By migrating subscriber data to datacenters it builds abroad, the provider could protect its subscribers from the reach of US law enforcement.[127] Another arbitrary means of circumvention occurs when a provider "move[s] data all over the world, sometimes breaking it into 'shards' so that different portions of a single email account may be stored in multiple countries at any one moment."[128] Google engages in such a technique, whereby it "automatically moves data from one location on Google's network to another as frequently as needed to optimize for performance, reliability, and other efficiencies."[129] Google's sharding method also makes it "possible that the network will change the location of data between the time when the legal process is sought and when it is served."[130] Indeed, "Google's compliance with a Section 2703 warrant would depend on the happenstance of where the data [are] located at the precise moment when the warrant is served or the provider accesses its network"[131] It therefore becomes extremely difficult to apply Microsoft's data location theory to other ISPs that have different methods for storing data. On the other hand, the Supreme

---

124. Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 202 (2d Cir. 2016). *See* Daskal, *supra* note 25, at 390; Brief for 51 Computer Scientists as Amici Curiae Supporting Respondent at 30, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2) ("While network latency is often measured in fractions of a second, these seemingly infinitesimal delays have dramatic effects. One study found, for example, 'that a half- second delay causes a 20 percent drop in traffic on Google, and a one tenth of a second delay can lower Amazon's sales by 1 percent'") (citing David Strom, *Layers of Latency: Cloud Complexity and Performance*, WIRED (Sept. 18, 2012), http://www.wired.com/2012/09/layers-of-latency/ [https://perma.cc/NA3C-WHGN]).

125. Daskal, *supra* note 25, at 390.

126. Brief for Petitioner at 15, United States v. Microsoft Corp., 138 S. Ct. 1186 (2017) (No. 17-2).

127. *Id.*

128. *Id.*

129. *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp.3d 708, 712 (E.D. Pa. 2017), *aff'd*, 275 F. Supp. 3d 605 (E.D. Pa. 2017).

130. *Id. But see* Brief for Respondent at 59–60, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2) (arguing that Google's architecture still renders data as having an ascertainable physical location, but Google was unable, in one case, to confirm the location of certain targeted communications) (citing Hearing Transcript 27, 40, *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-80263 (N.D. Cal. Aug. 10, 2017)).

131. Brief for Petitioner at 43, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2).

Court could have ruled on the specific facts of the *Microsoft* case and leave the issue open with regard to providers utilizing other data storage technologies, such as Google's.

Even Microsoft's former means of data storage were somewhat arbitrary because Microsoft's system used an automated process that depended upon information a subscriber provided, such as his or her "country code."[132] Besides Google and Microsoft, "some providers may not even be able to determine whether they currently store the requested data in the United States or abroad."[133] Although large providers may use automated processes, they still retain control and "may also have business incentives—based on customer demand—to move data to locations where cooperation with U.S. law enforcement is minimal, thus creating significant barriers for law enforcement agents investigating crimes."[134]

The next main problem pertains to burdening law enforcement. A Microsoft win would result in difficulty in conducting criminal investigations if law enforcement cannot obtain data that are stored abroad but maintained by a domestic provider.[135] Simply put, law enforcement would have to conduct investigations with less information. In our modernized world in which data contain a substantial amount of information, including evidence pertinent to criminal investigations, Microsoft's data location theory would create an "insurmountable barrier" to enforcing the law.[136] As a result, law

132. Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 829 F.3d 197, 210 (2d Cir. 2016). Unless manipulation occurs, this is no longer applicable to Microsoft's situation following its recent change in its data storage policy. *See* Brief for Respondent at 57, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2) (citing *Delivering a faster and more responsive Outlook.com*, MICROSOFT (Oct. 27, 2017), https://blogs.office.com/en-us/2017/10/27/delivering-a-faster-and-more-responsive-outlook-com/ [https://perma.cc/MZ8Y-JT7P]).

133. Brief for Petitioner at 44, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2).

134. Daskal, *supra* note 25, at 390. *But see* Brief for Respondent at 56, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2) (contending that Microsoft's decisions about where to store data was not based on evading or hampering law enforcement, but rather were based on reducing network latency).

135. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp, 15 F. Supp. 3d 466, 476-77 (S.D.N.Y. 2014); Brief for Petitioner at 41–45, United States v. Microsoft Corp., 138 S. Ct. 1186 (2017) (No. 17-2).

136. Brief for Petitioner at 15, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2).

enforcement would need to use diplomatic means to conduct investigations via the use of MLATs.[137]

An MLAT is an international agreement that allows for cooperation in criminal investigations and other related matters.[138] The MLAT process is extremely slow and complicated, and it begins with a formal request from law enforcement officials to another country for assistance and cooperation from that country with domestic law enforcement.[139]

The main problems surrounding MLATs stem from their procedures.[140] They are very slow and not universal, and MLAT requests can also be denied.[141] Typically, the entire MLAT process is estimated to last ten months or longer, depending in part on the number of requests.[142] Since 2000, MLAT requests have "increased nearly 85% and the number of requests for computer records has increased over 1000%."[143] MLATs "require the data to be held in a relatively fixed location, and in a location known to the United States."[144] This is extremely problematic and futile for data that move rapidly, such as that maintained by Google. MLATs are also not universal because the U.S. does not have an MLAT with every country in the world.[145] In the absence of an MLAT or executive agreement, Letters Rogatory could be another means to obtain cross-border assistance, but the entire process may take a year or more and has similar shortcomings as

137. *See Microsoft I*, 15 F. Supp. 3d at 474–75; Brief for Petitioner at 44–45, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2).

138. *See* 2 U.S. DEP'T OF STATE, INT'L NARCOTICS CONTROL STRATEGY REP.: MONEY LAUNDERING AND FIN. CRIMES 20 (Mar. 2012), https://www.state.gov/documents/organization/185866.pdf [https://perma.cc/C98T-LZWC].

139. For an overview of a typical MLAT process, see Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 749 (2016).

140. *See id.* at 748–51.

141. Brief for Petitioner at 44–45, Microsoft, 138 S. Ct. 1186 (No. 17-2); Daskal, *supra* note 25, at 393–94.

142. *Id. See* Daskal, *supra* note 25, at 393–94; *see also* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 409 (2014) ("[The MLAT] process generally remains slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other.").

143. CRIM. DIV., U.S. DEP'T OF JUSTICE, PERFORMANCE BUDGET: FY 2017 PRESIDENT'S BUDGET 23 (2016), http://www.justice.gov/jmd/file/820926/download [https://perma.cc/3AGB-YUCE].

144. Daskal, *supra* note 90.

145. *See* 2 U.S. DEP'T OF STATE, *supra* note 138, at 20; Daskal, *supra* note 25, at 394.

MLATs.[146] A final problem with the MLAT process is that an MLAT request may still be denied.[147] Therefore, such alternative measures to obtain stored data abroad are not currently the most efficient channels without some future legislative reform.

Furthermore, users can easily exacerbate the burden on law enforcement by manipulating the system, depending upon which provider they use, to ensure their data are stored abroad in order to evade law enforcement.[148] Users may subscribe to companies that store data outside the United States and in countries "unwilling, or perhaps technologically unable, to cooperate with official government-to-government requests for electronic evidence."[149] Another possible means of circumvention is for a user to simply input false information when signing up for an account or otherwise manipulating one's IP address to trick the provider's system to attribute the user's location to another country and, consequently, store that user's data abroad.[150] Moreover, a provider "is under no obligation to verify the information provided by a customer at the time an e-mail account is opened."[151] Microsoft subscribers, for example, were able to exploit the system using such methods, at least before its recent policy change.[152]

Ultimately, local and national security would also suffer if providers reduce cooperation with law enforcement in order to promote their own subscribers' interests and maintain a profitable business.[153] Barriers to law enforcement investigations "impinge[] on the ability to fight and solve crime," and this is likely to increase "as more and more

146. *See* U.S. DEP'T OF JUSTICE, LETTERS ROGATORY, CRIM. RESOURCE MANUAL 275, https://www.justice.gov/usam/criminal-resource-manual-275-letters-rogatory [http://perma.cc/R5DV-YHCZ]. *Contra* Matter of Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 210 (2d Cir. 2016) (referencing district court's concerns that "for countries with which it has not signed an MLAT, the United States has no formal tools with which to obtain assistance in conducting law enforcement searches abroad").

147. *See In re* A Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 474 (S.D.N.Y. 2014).

148. Daskal, *supra* note 25, at 390.

149. *Id.*

150. Brief for Petitioner at 11, *Microsoft Corp*., 138 S. Ct. 1186 (No. 17-2). *See* Roland Waddilove, *How to use a VPN*, TECH ADVISOR (June 20, 2018), https://www.techadvisor.co.uk/how-to/internet/how-use-vpn-3466190/ [https://perma.cc/3HDM-B7RT] (explaining Virtual Private Networks and how they can "make it appear as if [a user is] located in another country").

151. *Microsoft I,* 15 F. Supp. 3d at 474.

152. Brief for Petitioner at 11, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).

153. *See* Daskal, *supra* note 25, at 390.

evidence becomes digitalized, even in run-of-the-mill local crimes."[154] On a national level, national security combating terrorism would also be at risk, especially considering the global nature of modern terrorism.[155] In fact, following the Second Circuit's decision, law enforcement divisions have already experienced some difficulties in investigations.[156]

A final overarching issue with a Microsoft win would be that it may also fuel data localization movements. A Microsoft win with such an outcome would seem almost irreconcilable with a government win: How could both possible outcomes of the Microsoft decision lead to the same problem? There are nuances to both data localization movements that slightly differentiate them, that help address this conundrum. Unlike data localization movements previously described,[157] movements responding to a Microsoft win would target providers, rather than nationals, and regulate server location, rather than provider location.[158] If the physical location of a server determines law enforcement's access to stored data, nations mandating data localization laws would "require data collecting Internet companies to store the collected data on servers physically located within [their own] country."[159]

Some providers that aim to protect their users and avoid the grasp of US law enforcement might even voluntarily migrate their stored data to a location abroad—data localization initiated by a provider itself rather than a nation's government.[160] Even though there are differences between these data localization movements, some of the effects are the

154. Daskal, *supra* note 36, at 480.

155. *See* Brief for Petitioner at 11, 41, *Microsoft Corp.*, 138 S. Ct. 1186 (No. 17-2).

156. *See* Benjamin Battles, *Business decisions should not control whether law enforcement can investigate local crimes*, SCOTUSBLOG (Feb. 6, 2018, 10:25 AM), http://www.scotusblog.com/2018/02/symposium-business-decisions-not-control-whether-law-enforcement-can-investigate-local-crimes/ [https://perma.cc/9Z5C-CLHP] (citing impeded investigations involving crimes against minors in Vermont, Utah, and California); *Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Statement Before the Comm. On the Judiciary,* 115th Cong. 5-6 (2017) (statement of Richard W. Downing, Acting Deputy Assistant Att'y Gen.) [hereinafter Downing Statement] (citing several examples of impeded investigations).

157. *See supra* Part III.A.

158. *See generally* Daskal, *supra* note 25, at 392 (differentiating data localization movements).

159. Hsiao, *supra* note 40, at 219. *Accord* Woods, *supra* note 139, at 751.

160. *See* Daskal, *supra* note 36, at 488.

same, such as efficiency costs affecting network speeds and monetary costs on providers that would spread to users.[161] Apple, for instance, recently announced that it will begin to store iCloud account information of its Chinese subscribers in China as part of a joint venture with a Chinese partner.[162] This is a result of new data localization laws requiring "cloud services offered to Chinese citizens [to] be operated by Chinese companies and that the data be stored in China."[163] Chinese officials will be able to use their own legal system to get access to Apple's Chinese subscriber information instead of going to US courts. This raises concerns about potential human rights abuses, such as the Chinese government using this more easily accessible information to track down dissidents.[164]

Localization efforts could also theoretically drive law enforcement officers to "resort to other, less wholesome tactics to get access" to data stored abroad.[165] For example, such tactics may include raiding the offices of providers and even surveilling a nation's own citizens.[166] Other adverse implications involve "the innovative potential of the Internet and . . . privacy rights of both American and foreign-based users."[167] Specifically, Americans with data stored abroad will be at risk for privacy intrusions if that nation does not have as high a standard as probable cause in obtaining a lawful warrant.[168] Small start-ups may also get priced out of the international market if foreign nations with localization laws source only from domestic ISPs.[169]

161. *See* Woods, *supra* note 139, at 752–53.

162. Stephen Nellis & Cate Cadell, *Apple moves to store iCloud keys in China, raising human rights fears*, REUTERS (Feb. 24, 2018, 12:14 AM), https://www.reuters.com/article/us-china-apple-icloud-insight/apple-moves-to-store-icloud-keys-in-china-raising-human-rights-fears-idUSKCN1G8060 [https://perma.cc/67KS-7H3K].

163. *Id.*

164. *Id.*

165. Woods, *supra* note 139, at 751.

166. *Id.* at 751, 753.

167. *See* Daskal, *supra* note 36, at 488.

168. *Id.*

169. Daskal, *supra* note 90.

V. PROPOSAL

The previous discussion demonstrates the difficulty posed by *Microsoft* and the state of the law before passage of the CLOUD Act.[170] Fortunately, Congress has recently passed legislation that specifically addresses the extraterritoriality problems. Part V discusses the challenges to the extraterritorial framework as well as the CLOUD Act as a solution.

A. The Difficulty of Framing Data Territorially

The debate about whether data has features of territoriality and can be subject to rules of territoriality largely depends on how one describes data's characteristics. On the one hand, data are territorial and have features of both intangible assets (like intellectual property, investments, and debts) and physical assets.[171] Accordingly, courts "have at least two lines of inquiry for determining when a state ought to be able to properly assert jurisdiction over data in the cloud": it can properly apply existing case law dealing with either intangible or physical assets to data.[172] The other side of the debate is more persuasive, finding that data have unique characteristics that "raise fundamental challenges to territoriality doctrine."[173] Declaring that data can be assigned to a physical location is arbitrary because data move frequently, and sometimes in pieces, depending on the providers' algorithms and business decisions, and typically without any consent or even awareness on behalf of the user.[174] Although it would be convenient, the concept of data simply is an exceptional phenomenon and should be treated according to its own characteristics—not the characteristics of anything else.

Framing the issue of the government's ability to access data stored abroad in territorial terms brings with it practical difficulties as well as negative results, either way. One commentator succinctly pointed out some of these issues:

---

170. *See supra* Parts III–IV.

171. *See* Woods, *supra* note 139, at 734–35, 756–63 (arguing that data does not have novel features, but instead is inherently territorial, and courts may treat it as an intangible asset or as a physical object).

172. *Id.* at 763.

173. Daskal, *supra* note 25, at 378.

174. *See id.* at 367, 373.

> Territorial rules aspire to certainty, but technology makes it harder to define "territoriality" in a consistent and predictable way. Technology weakens territoriality as a proxy for policy goals because data often move in ways that are disconnected with the interests of users and lawmakers. Technology makes it easier for public and private actors to circumvent territorial rules (often without detection), thus interfering with the existing allocation of policymaking authority.[175]

B. Building on the CLOUD Act

Microsoft illustrates the difficulties that come with outdated laws that vaguely address an issue. In its unamended state, the SCA would not give a satisfactory answer to the question of whether providers must comply with SCA warrants when law enforcement seeks data stored abroad.[176] Shortly before the *Microsoft I* decision came out, Microsoft wrote in a blog post that having "[c]learer rules for access to data

---

175. Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 46 (2016).

176. Orin Kerr proposed an alternative to applying the SCA to *Microsoft*. Kerr argues that Microsoft should have made its challenge under the All Writs Act instead of the SCA. Orin Kerr, *Microsoft Challenged the Wrong Law. Now What?*, LAWFARE (Nov. 27, 2017), https://www.lawfareblog.com/microsoft-challenged-wrong-law-now-what [https://perma.cc/48DF-D9FY]. He analogizes the Microsoft situation as analogous to United States v. New York Telephone Co., 434 U.S. 159 (1977), in which the Supreme Court held that federal courts may issue assistance orders under the authority of the All Writs Act to compel a communications provider, "as may be necessary or appropriate to effectuate" a warrant. An AWA framework would provide better results, Kerr asserts, because it would avoid the two poor results stemming from Microsoft's current SCA framework. Kerr, *supra* note 176. Instead, the AWA would empower judges to use their discretion and create more flexible judge-made rules, leading to more sensible outcomes. *Id.*

Jennifer Daskal directly challenges Kerr's theory. *See* Jennifer Daskal, *Why Microsoft Challenged the Right Law: A Response to Orin Kerr*, JUST SECURITY (Dec. 8, 2017), https://www.justsecurity.org/48907/microsoft-challenged-law-response-orin-kerr/ [https://perma.cc/ZSZ4-D4EC]. Daskal argues that the SCA is the key issue, not the AWA. The government, Microsoft, and "every judge that has looked at the issue" have framed it as an SCA case. Daskal notes that the SCA deals with "the kind of compelled disclosure warrants at issue in the case" and that Kerr relies on pre-SCA cases that are distinguishable from the circumstances at play in *Microsoft*. *Id.* The AWA "is a residual source of authority to issue writs that are not otherwise covered by statute. Where a statute specifically addresses the particular issue at hand, it is that authority, and not the All Writs Act, that is controlling." Carlisle v. United States, 517 U.S. 416, 429 (1996) (quoting Pennsylvania Bureau of Correction v. United States Marshals Service, 474 U.S. 34, 43 (1985)). Finally, Daskal states that the AWA framework still begs the question of whether "this a territorial or extraterritorial exercise of the government's warrant authority." Id. I agree with Daskal that the SCA, rather than the AWA, applies in *Microsoft*.

internationally would help open borders and enable companies to host services and data in one country for citizens in another."[177] The need for a bright-line rule was evident. Microsoft summarily pointed out that Congress should legislate and "rewrite the statute to strike a new, twenty-first century balance between law-enforcement interests, our relations with foreign nations, the privacy of our citizens, and the competitiveness of our technology industry,"[178] a belief that the government also shares, albeit with a much stronger emphasis on law-enforcement interests.[179]

On February 6, 2018, Senator Orrin Hatch introduced a bill to directly address the issue, and it is aptly entitled the CLOUD Act.[180] This bipartisan bill is supported both by the US Department of Justice and large technology companies, including Microsoft.[181] During his introduction of the bill, Senator Hatch acknowledged the need to legislate, noting the negative consequences of either outcome of *Microsoft*.[182] Specifically, he stated that "[n]o matter how the Court

177. *Time for an international convention on government access to data*, MICROSOFT CORP. BLOGS (Jan. 20, 2014), https://blogs.microsoft.com/on-the-issues/2014/01/20/time-for-an-international-convention-on-government-access-to-data/ [https://perma.cc/5CEW-CT5E].

178. Brief for Respondent at 14, United States v. Microsoft Corp., 138 S. Ct. 1186 (2018) (No. 17-2).

179. The Department of Justice announced six principles that it thinks should be implemented in a new solution. Downing Statement, *supra* note 156, at 9–10. The principles are as follows: (1) "a solution must permit law enforcement investigators effectively to obtain digital evidence without undue delay"; (2) "reliance solely on the MLA[T] process cannot be the solution"; (3) "a solution cannot grant foreign governments a veto authority over U.S. criminal investigations," with China and Russia in mind; (4) "a solution must take into account the reality that investigators often will not know the identity, nationality, or location of the account holder"; (5) "a solution should avoid creating an incentive for other countries to create 'data localization' laws"; and (6) "a solution should not grant benefits or protections to foreigners that are not also granted to U.S. citizens and residents." *Id.*

180. CLOUD Act.

181. Jennifer Daskal, *Justices can, and should, write nuanced ruling to balance competing interests*, SCOTUSBLOG (Feb. 7, 2018, 10:35 AM), http://www.scotusblog.com/2018/02/symposium-justices-can-write-nuanced-ruling-balance-competing-interests/ [https://perma.cc/4Y2A-FDR8]. *See* Letter from Apple, Facebook, Google, Microsoft, & Oath to Sens. Orinn Hatch, Christopher Coons, Lindsey Graham, & Sheldon Whitehouse (Feb. 6, 2018), https://blogs.microsoft.com/datalaw/wp-content/uploads/sites/149/2018/02/Tech-Companies-Letter-of-Support-for-Senate-CLOUD-Act-020618.pdf [https://perma.cc/4D6D-V5F2] [hereinafter Company Letter of Support].

182. Press Release, Orrin Hatch, Hatch Previews CLOUD Act: Legislation to Solve the Problem of Cross-Border Data Requests, (Feb. 5, 2018) [hereinafter Press Release, Orrin Hatch], https://www.hatch.senate.gov/public/index.cfm/2018/2/hatch-previews-cloud-act-legislation-to-solve-the-problem-of-cross-border-data-requests [https://perma.cc/8BMZ-VGTS].

rules . . . problems will remain. Either law enforcement will lack the ability to obtain in a timely manner email and documents in the cloud that are stored overseas, or providers will find themselves caught between conflicting domestic and foreign laws."[183] Congress passed the CLOUD Act on March 23, 2018.[184] Although not without some concerns, the CLOUD Act improves upon the status quo—an outdated statute that does not clearly address the *Microsoft* issue and would lead to one of two negative outcomes.[185]

The CLOUD Act has two main parts.[186] The first part addresses the *Microsoft* issue head on, stating that a provider must comply with SCA warrants if the information sought is "within such provider's possession, custody, or control, regardless of whether such communication, record, or other information is located within or outside of the United States."[187] This provision makes it the default for a provider to comply with government requests for data stored abroad. There is an exception to the default, which is for a provider to file a motion to quash or modify if, in a particular instance, the provider reasonably believes the target of the government request is a customer or subscriber who "is not a United States person and does not reside in the United States" and, secondly, "that the required disclosure would cause the provider to violate the laws of a qualifying foreign government," which is a government with which the United States has an executive agreement.[188] The government is given an opportunity to respond and the court may modify or quash if it finds the disclosure would violate the foreign country's law, if the target is not a US citizen or resident, and if it would be in the interests of justice.[189] The last factor requires the court to conduct a comity analysis, which may be helpful guidance for a court, but it may also be more of a "symbolic gesture" of good will towards other countries.[190]

---

183. *Id.*

184. CLOUD Act, 1212.

185. *See supra* Parts III-IV.

186. Sen. Hatch conceptualizes the bill has having four key components. For his breakdown of the bill, *see* Press Release, Orinn Hatch, *supra* note 182.

187. CLOUD Act § 103(a)(1).

188. CLOUD Act § 103(b).

189. *Id.*

190. Andrew Keane Woods & Peter Swire, *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 [https://perma.cc/ZK6X-CTVQ] ("[C]ourts were already free under the common law to conduct a comity analysis in thinking

The second main part of the CLOUD Act lifts the blocking provisions of the SCA, meaning that ISPs are permitted to comply with certain foreign government requests for data if an executive agreement between the United States and that country exists.[191] Under the current SCA, foreign governments cannot directly request data from US-based providers, but must instead go through diplomatic channels, "enlist[ing] the help of the US Department of Justice to compel the US providers to turn over evidence even if the crime being investigated is wholly domestic."[192] The bill then lays out the procedures for creating executive agreements while also answering the question of how a foreign country can become a "qualifying foreign government," which is a required condition for a provider to object to disclosing information, by filing a motion to quash or modify under the first part of the bill.[193] To become a qualifying foreign government, a foreign country must adhere to certain international human rights standards and have sufficient substantive and procedural protections for accessing data, including minimization procedures for the "dissemination of information concerning U.S. persons."[194] Additionally, the foreign government is prohibited from intentionally targeting a US person or a person located in the United States either directly or indirectly.[195] Once the US Attorney General makes a determination about whether to enter into an executive agreement with a country, that decision is not subject to any kind of judicial or administrative review.[196]

Microsoft and other technology companies have endorsed the CLOUD Act because they believe it balances differing interests of law

---

through whether to issue an order with extraterritorial impact. Its presence in the statute is perhaps a reminder that trust and mutual respect play an important role in these cross-border matters."). *But see* Jennifer Daskal, *New Bill Would Moot Microsoft Ireland Case—And Much More!*, JUST SECURITY (Feb 6, 2018), https://www.justsecurity.org/51886/bill-moot-microsoft-ireland-case-more/ [https://perma.cc/5GZL-WDTS] (The bill "explicitly preserves, via a rule of construction, the availability of common law comity claims in situations involving non-qualifying countries. . . . It thus preserves the availability of providers to raise comity claims even in situations where there is not explicit statutory authority to do so—and move to quash based on the fact that the execution of warrant will generate a conflict of laws.").

191. CLOUD Act § 4.

192. Alex Grigsby, *The Intelligence Collection Implications of the CLOUD Act*, COUNCIL ON FOREIGN RELATIONS BLOG POST (Feb. 12, 2018), https://www.cfr.org/blog/intelligence-collection-implications-cloud-act [https://perma.cc/Q7AB-MHS2].

193. CLOUD Act § 3(b).

194. CLOUD Act § 5(a).

195. *Id.*

196. *Id.*

enforcement, customer privacy, and "gives the technology sector two distinct statutory rights to protect consumers and resolve conflicts of law," which include "mechanisms to notify foreign governments when a legal request implicates their residents, and to initiate a direct legal challenge when necessary."[197]

Opponents of the CLOUD Act, largely consisting of privacy and human rights organizations,[198] are primarily concerned about the effects of diminished privacy and the potential for abuse.[199] Camille Fischer, a former Obama administration policy advisor and current Electronic Frontier Foundation fellow, was concerned about the fact that "the bill would allow the President to enter into 'executive agreements' with foreign governments that would allow each government to acquire users' data stored in the other country, without following each other's privacy laws."[200] These concerns are for the privacy interests of people the bill does not explicitly protect—people who are not US persons or persons located in the United States.[201] A government win in *Microsoft* would have afforded zero protection to any person, regardless of nationality, because the interpretation would have centered around the custody and control of the sought-after data.[202] At least with the CLOUD Act, U.S. citizens are afforded a stronger guarantee of privacy than could previously have been the case.

197. Company Letter of Support, *supra* note 181.

198. Neema Singh Guliani, *The Cloud Act Is a Dangerous Piece of Legislation*, ACLU (Mar. 13, 2018), https://www.aclu.org/print/node/67581 [https://perma.cc/9RYE-5ZSC].

199. *See* 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 [https://perma.cc/P64V-83NH]; Derek B. Johnson, *New CLOUD Act splits industry, civil liberty orgs*, FCW (Feb. 9, 2018), https://fcw.com/articles/2018/02/09/cloud-act.aspx [https://perma.cc/SD54-K66N].

200. Fischer, *supra* note 199.

201. *Id. See* Johnson, *supra* note 199 ("The Center for Democracy and Technology, a think tank focused on Internet freedom issues, also has come out against the legislation, arguing the new version would allow the Department of Justice to authorize foreign governments to demand wiretaps on U.S. companies absent a warrant."); Grigsby, *supra* note 192 ("Although the bill ostensibly aims to help foreign countries obtain data to investigate local crimes, it could also make it easier for them to collect data from U.S. providers for intelligence purposes on targets anywhere in the world.").

202. *See* Brief for Petitioner at 16, 31, United States v. Microsoft Corp., 138 S. Ct. 1186 (2017) (No. 17-2).

Opponents also find that the bill does not afford sufficient Fourth Amendment protections.[203] Specifically, the language in the statute is too vague, as it "provides only *factors*, *not requirements*, for approval and is written so broadly as to be open to interpretation."[204] Because the standard is worded somewhat ambiguously, this gives the U.S. government more discretion in its decisions and will likely result in less transparency or accountability, especially considering the lack of judicial review.[205] The concerns about transparency are well founded and Congress should consider amending the CLOUD Act.

The ACLU also calls the bill a threat to "global activists."[206] They state that, under the current standard, activists' information abroad is "protected from being disclosed by U.S. companies to governments who may seek to do them harm."[207] However, the CLOUD Act would "eliminate[] many of these protections and replace[] them with vague assurances, weak standards, and largely unenforceable restrictions."[208] Although the Attorney General must consider the enumerated factors, "he is not *prohibited* from entering into an agreement with a country that has committed human rights abuses."[209] Even Daskal, a proponent of the CLOUD Act, agrees that the executive agreement approval process could be strengthened and also made transparent, and possibly subject to some third party oversight.[210]

---

203. *See* David Ruiz, *A New backdoor around the Fourth Amendment: The CLOUD Act*, ELECTRONIC FRONTIER FOUND. (Mar. 13, 2018), https://www.eff.org/deeplinks/2018/03/new-backdoor-around-fourth-amendment-cloud-act [https://perma.cc/VGS4-42YE] (arguing that foreign law enforcement will be able to collect Americans' communications and share them with the U.S. government under the vaguely worded 'significant harm' test and that the U.S. government may use this information against Americans without first obtaining probable cause or a search warrant); Fischer, *supra* note 199; Grigsby, *supra* note 192.

204. Drew Mitnick, *A diagnosis: Why current proposals to fix the MLAT system won't work*, ACCESS NOW (May 2, 2017) (emphasis added), https://www.accessnow.org/diagnosis-current-proposals-fix-mlat-system-wont-work/ [https://perma.cc/6SJK-C6SP]. *See* CLOUD Act § 105(a) (setting out the "factors to be considered" by the executive branch in determining whether to enter into an executive agreement).

205. *See* Mitnick, *supra* note 204.

206. Guliani, *supra* note 198.

207. *Id.*

208. *Id.*

209. *Id.*; *see* Ruiz, *supra* note 203.

210. Jennifer Daskal & Peter Swire, *Why the CLOUD Act is Good for Privacy and Human Rights*, LAWFARE (Mar. 14, 2018), https://lawfareblog.com/why-cloud-act-good-privacy-and-human-rights [https://perma.cc/XW44-RCE7].

The CLOUD Act was rightfully enacted before the Supreme Court ruled on the matter. Congress was correct to adopt this legislation because it addresses the contested issue in *Microsoft* and appears to adequately balance the competing interests involved. The unamended version of the SCA was wholly insufficient to deal with the technological realities of today. However, certain parts of the CLOUD Act should be modified. The CLOUD Act should be subject to four main changes.

First, transparency should be required in creating executive agreements with regard to the CLOUD Act. Currently, the executive agreements within the CLOUD Act are "not [] subject to judicial or administrative review,"[211] but Congress can still check the executive. The Attorney General must notify Congress within seven days of certifying an executive agreement.[212] Then, the agreement enters into force no earlier than 180 days after notice, unless Congress enacts a joint resolution of disapproval.[213] Such a check on the executive agreement only appears to rest with Congress as there is no provision requiring the exact terms of the agreement to be disclosed. One commentator of the CLOUD Act, Greg Nojeim, pointed out concerns about such lack of transparency because the Justice Department has not disclosed the contents of a draft agreement with the United Kingdom made before the CLOUD Act, nor has it disclosed which countries have approached the United States about entering into such agreements.[214] Although the government's actions in these examples may be predictive, they are not determinative of what the government will actually do when a final agreement is reached. These concerns focus on the negotiating stages of such executive agreements. However, until the first CLOUD Act executive agreement is reached, the government's position on the transparency of the details of the agreement is speculative.

---

211. CLOUD Act § 105(c).

212. CLOUD Act § 105(d).

213. CLOUD Act § 105(d). A joint resolution of disapproval can be introduced in either the House of Representatives or the Senate. CLOUD Act § 105(d). It also requires approval by both houses of Congress and by the President or else both houses must override a presidential veto. *See* 7 Deschler's Precedents of the United States House of Representatives 4791 (1994).

214. Greg Nojeim, *Cloud Act Implementation Issues*, LAWFARE (July 10, 2018, 8:00 AM), https://www.lawfareblog.com/cloud-act-implementation-issues [https://perma.cc/Y9HY-R5GF].

Transparency acts as a check on the executive branch, ensuring that its decisions are thoroughly and thoughtfully considered.[215] Similar to how courts issue opinions, a determination about an executive agreement can be reported and explained.[216] This way, decisions are subject to public and media scrutiny. Additionally, if an applicant country is denied, that country is given an explanation and, if it so desires, may make certain changes to be in compliance for a subsequent application. Transparency will also ensure that decisions are not based on unrelated political factors, such as an historically good or bad relationship with a certain country or political retaliation or advantage, among other reasons. Determinations about executive agreements should focus on the factors listed in the CLOUD Act and avoid being overly influenced by politics.

If the executive branch enters into an agreement with a country that commits human rights abuses, there should be some recourse for targets of CLOUD Act warrants or disclosure requests by foreign nations.[217] Executive agreements that are publicly available may also be used by targets of a CLOUD Act warrant or disclosure request by a foreign nation to challenge whether there is an applicable executive agreement. Such valid challenges could not effectively take place without knowing the contents of the applicable executive agreement, if one exists.

Secondly, under the current CLOUD Act, providers are not required to disclose the existence of legal process to a foreign government.[218] Specifically, providers are not in violation of the Act if they "disclose to the entity within a qualifying foreign government . . .

---

215. *See* WENDY GINSBERG, CONG. RESEARCH SERV., R42817, GOVERNMENT TRANSPARENCY AND SECRECY: AN EXAMINATION OF MEANING AND ITS USE IN THE EXECUTIVE BRANCH 30 (2012) (quoting OFFICE OF MGMT. & BUDGET, EXEC. OFFICE OF THE PRESIDENT, MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES: OPEN GOVERNMENT DIRECTIVE 1 (2009)).

216. The executive branch must submit a written certification to Congress explaining how the requirements for an executive agreement have been met. CLOUD Act § 105(d). However, there is no requirement that certification be public.

217. The earlier version of the CLOUD Act listed human rights criteria as certain "factors to be considered," whereas the enacted version states them as "factors to be met." Sharon Bradford Franklin, *The Forecast Is Still Cloudy*, SLATE (Mar. 29, 2018, 3:36 PM), https://slate.com/technology/2018/03/the-cloud-act-could-hurt-human-rights-around-the-world.html [https://perma.cc/MK64-XSZM] (internal quotation marks omitted).

218. CLOUD Act § 103(h)(5).

the fact of the existence of legal process."[219] Instead of giving providers the discretion of whether or not to disclose, the Act should instead require such disclosure to an appropriate authority of every government, qualifying or non-qualifying. An appropriate authority would likely be the equivalent of the US Department of Justice. This aids in transparency and provides more trust between the United States and other governments. Additionally, such a requirement would necessarily come with a punishment for providers that do not disclose. Since the purpose is not to punish providers, but rather to ensure transparency, such a punishment could consist of a fine.

Third, there should be an additional section updating the MLAT process for non-qualifying countries. If no executive agreement exists, then such countries are left with the old MLAT process that remains slow and not universal.[220] As the CLOUD Act currently stands, it appears to disregard the preferred policies of other countries solely based on whether or not an executive agreement with the United States exists.[221] The qualifying/non-qualifying distinction should remain, but there should still be some sort of recourse for countries without an executive agreement that have a valid interest and objection to the legal process. Thus, although a provider is not required to file a motion to quash or modify, the provider would be required to notify both qualifying and non-qualifying foreign governments of the legal process, under the second proposed change. With that notification, the non-qualifying country itself could file an objection or a motion to suspend until the MLAT process has been fully carried out.

Finally, the CLOUD Act currently only allows a court to modify or quash legal process if it finds that three conditions are fully met.[222] The first condition is that the "required disclosure would cause the provider to violate the laws of a qualifying foreign government."[223] The second condition allows modification if, "based on the totality of the circumstances, the interests of justice dictate that legal process should be modified or quashed" after conducting the comity analysis.[224] The

219. *Id.*

220. *See supra* notes 138-47 and accompanying text.

221. Only a provider may file a motion to quash or modify and the filing of this motion is conditioned upon there being a material risk that the required disclosure would cause the provider to violate the laws of a "qualifying foreign government." CLOUD Act § 103(a)(1).

222. CLOUD Act § 103(a)(2)(b).

223. *Id.*

224. *Id.*

third and final condition is that "the customer or subscriber is not a United States person and does not reside in the United States."[225]

Considering the second and third recommended modifications regarding notification to all countries and allowing non-qualifying countries to make an objection, the conditions about when a court may modify or quash legal process should also be adjusted. The second and third conditions for quashing legal process may be left the same. However, the problem with the first condition is that, at least initially, not many countries will have an executive agreement with the United States, and, thus, it would be impossible to modify or quash any legal process if that non-qualifying country is involved. Another issue with this condition is that a legal process may not necessarily violate the laws of another country, but it could cause outrage that may incite that country's government to retaliate with data localization laws. Preventing data localization is in the interest of both law enforcement and a provider and should consequently be of the utmost importance.

Instead of being a required condition, the first factor that the "required disclosure would cause the provider to violate the laws of a qualifying foreign government" should be an optional finding.[226] Also, an additional optional finding should be that a non-qualifying country has submitted a valid MLAT request (under a revised MLAT system), and in that case, the court may also suspend the order temporarily, pending the completion of the revised MLAT process. Such a reading would give a judge more discretion in deciding such motions, also helping to balance the executive branch's power to enter into executive agreements and thereby dictate which countries are "qualifying" as well as to respect other countries' rules of law.[227]

VI. CONCLUSION

Prior to the enactment of the CLOUD Act, the SCA was incapable of adequately addressing all of the competing interests that were at play in *Microsoft*. The CLOUD Act is a solution that takes into account the technological reality of today that is increasingly transcending physical borders. It is a legislative attempt to appease law enforcement, providers, users, and foreign nations. For now, it provides a solid

225. *Id.*
226. *Id.*
227. *Id.*

foundation, and with certain modifications, it could be a promising solution.