Fordham Law Review

Volume 86 | Issue 4 Article 16

2018

Beyond *Microsoft*: A Legislative Solution to the SCA's Extraterritoriality Problem

Andrew Kirschenbaum
Fordham University School of Law

Beyond *Microsoft*: A Legislative Solution to the SCA's Extraterritoriality Problem

Erratum

Law; Criminal Law; Legislation; Computer Law; Criminal Procedure; Computer Law; Fourth Amendment

BEYOND *MICROSOFT*: A LEGISLATIVE SOLUTION TO THE SCA'S EXTRATERRITORIALITY PROBLEM

*Andrew Kirschenbaum**

The Stored Communications Act governs U.S. law enforcement's access to cloud data, but the statute is ill equipped to handle the global nature of the modern internet. A pending U.S. Supreme Court case, United States v. Microsoft, *raises the question whether a warrant under the statute may be used to reach across international borders to obtain data that is stored in another country, regardless of the user's nationality. While the Court will determine whether this is an impermissible extraterritorial application of the current law, many have called for a legislative resolution to this issue.*

Due to the insufficiency of the current law, the limits of traditional judicial doctrines, and the inherent advantages the legislature has over the judiciary in addressing technological change, this Note also recommends a legislative resolution. Building upon a legislative proposal, this Note proposes a framework with two separate sets of legal procedures based on user identity. These separate domestic and extraterritorial procedures provide a framework that would set clear guidelines for law enforcement and service providers while giving due respect to foreign sovereignty.

INTRODUCTION 1925

I. BACKGROUND 1928

A. The Current Technological Context: Cloud Storage and International Data Regulation 1928

1. The Cloud and Network Architecture 1929

2. Maintaining Local Control of Data: Data Localization and International Privacy Concerns 1930

B. Judicial Privacy Protection: Constitutional Limits to Searches and Seizures Abroad and in the Cloud 1931

1. Warrants, the Fourth Amendment, and Global Data Storage 1932

* J.D. Candidate, 2019, Fordham University School of Law; B.A., 2009, The College of New Jersey. I would like to thank Professor Olivier Sylvain for his guidance and encouragement and the editors and staff of the *Fordham Law Review* for their assistance and hard work. I would also like to thank my wife Devon, my parents, Caitlin, Chris, and all of my family and friends whose support over the years made this Note possible.

2. Subpoenas and Extraterritoriality 1935
C. Statutory Privacy Protection: The Stored Communications Act 1936
1. A Brief History of the SCA 1937
2. The SCA's Warrant Provision 1938
D. What's Extraterritorial When It Comes to the SCA?: Microsoft I *and Its Rebellious Progeny* 1939
1. *Microsoft I* 1940
2. *Microsoft II* Dissents and the District Courts 1942
a. Warrant-Subpoena Hybrid View 1943
b. Fourth Amendment Search-but-Not-Seizure View 1944
c. Distinguishing the Google Cases from Microsoft I *on the Facts* 1946
II. THE POSSIBLE OUTCOMES OF *MICROSOFT* AND CALLS FOR LEGISLATIVE ACTION 1947
A. The Supreme Court's Limited Options in Microsoft 1947
1. Holding for Microsoft 1948
2. Holding for the Government 1948
3. A Possible Solution Under the All Writs Act 1949
B. The Advantages of a Legislative Solution 1950
C. Envisioning the SCA's Replacement 1951
1. Service Providers Call for a Nuanced Legislative Solution 1952
2. Law Enforcement Officers Call for Clarity 1952
D. Proposed Legislation: The International Communications Privacy Act 1954
III. A LEGISLATIVE SOLUTION THAT SEPARATES DOMESTIC AND FOREIGN SEARCHES ON THE BASIS OF USER IDENTITY 1957
A. What the ICPA Gets Right and What It Lacks 1958
B. Governing Access to United States and Foreign User Data with Fully Separate Procedures 1958
1. The Domestic Warrant 1959
2. The International Order 1959
3. The Warrant and International Order System: Benefits of Separate Procedures 1960
CONCLUSION 1961

INTRODUCTION

The Stored Communications Act (SCA), passed more than thirty years ago as Title II of the Electronic Communications Privacy Act (ECPA),[1] governs rapidly advancing technology.[2] The SCA is widely viewed as outdated.[3] The statute was originally passed to protect the privacy of electronic communications that were not clearly protected by the Fourth Amendment.[4] The SCA prohibits service providers[5] from releasing electronic communications except under certain circumstances.[6] The statute also provides procedures for law enforcement to compel the release of communications.[7]

Courts have struggled to apply the SCA to changing technology.[8] In particular, applying the SCA's warrant provision[9] to the contents of communications that can be moved and electronically stored all over the globe has posed a challenge.[10] The question whether the warrant provision of the SCA would allow U.S. law enforcement officials to obtain electronic data stored on overseas servers, sometimes in fragmented form, was unforeseeable in 1986. However, this once unforeseeable question was addressed by the Second Circuit in *Microsoft Corp. v. United States* (*In re*

1. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

2. 18 U.S.C. §§ 2701–2712 (2012).

3. *See, e.g.*, Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 231–33 (2d Cir. 2016) (Lynch, J., concurring) (noting the need for Congress to modernize the SCA), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2); International Communications Privacy Act, S. 1671, 115th Cong. (2017) (proposing amendments to the SCA); Brad Smith, *A Legislative Path to Create New Laws Is Better than Arguing Over Old Laws*, MICROSOFT ON ISSUES (June 23, 2017), https://blogs.microsoft.com/on-the-issues/2017/06/23/legislative-path-create-new-laws-better-arguing-old-laws/ [https://perma.cc/2YHW-U5KZ]; *see also infra* Part II.C.

4. *See In re* Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 145 (3d Cir. 2015) ("[T]he Stored Communications Act was born from congressional recognition that neither existing federal statutes nor the Fourth Amendment protected against potential intrusions on individual privacy arising from illicit access to 'stored communications in remote computing operations and large data banks that stored e-mails.'" (quoting Garcia v. City of Laredo, 702 F.3d 788, 791 (5th Cir. 2012))); Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 400 (2014) ("Congress intended [the SCA] as a stopgap measure designed to impose statutory protections until Fourth Amendment precedents became established.").

5. This Note will use the terms "service provider" and "provider" as shorthand for providers of the two services the SCA protects, electronic communication services (ECS) and remote computing services (RCS). These services are less distinguishable now than they were when Congress passed the SCA in 1986, and the providers under discussion in this Note generally supply both kinds of services. *See Microsoft I*, 829 F.3d at 206–07; Kerr, *supra* note 4, at 397; *see also infra* notes 127–29.

6. *See* 18 U.S.C. § 2702(a); *see also* Kerr, *supra* note 4, at 383.

7. *See* 18 U.S.C. § 2703; *see also* Kerr, *supra* note 4, at 383.

8. *See, e.g.*, *Microsoft I*, 829 F.3d at 210–22; *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 717–22 (E.D. Pa.), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017); *see also* Kerr, *supra* note 4, at 390–410 (describing technological and legal changes since the SCA was passed in 1986 that have made the SCA and ECPA outdated).

9. 18 U.S.C. § 2703(a)–(b)(1)(A).

10. *See, e.g.*, *Microsoft I*, 829 F.3d at 209.

Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*)[11] and is currently being considered by the U.S. Supreme Court.[12] The issue in the case is whether it is an impermissible extraterritorial application of the SCA's warrant provision for the government to compel a private party's retrieval and production of email content from overseas servers.[13] The case also raises an even more fundamental question: what branch of the government is best equipped to address these problems?[14]

Due in part to the limited language within the SCA, courts that have considered this question have come to conclusions that are all or nothing: either an SCA warrant has the potential to reach across borders to obtain the data of foreign citizens[15] or its reach is arbitrarily limited by where a company stores its users' data.[16] In some cases, the latter conclusion would result in situations where U.S. law enforcement officials have indisputable probable cause to justify access to a U.S. citizen's communications yet cannot obtain the records solely because of the provider's choice of storage location.[17] Meanwhile, placing no limit on the unilateral ability of U.S. law enforcement to use U.S.-based providers to retrieve data stored in a foreign country implicates international comity and may subject providers to conflicts of law.[18] The potential ramifications are unsatisfactory to service providers,[19] law enforcement,[20] and judges alike.[21]

---

11. 829 F.3d 197 (2d Cir. 2016).

12. Oral arguments in this case are set for February 27, 2018. *Docket No. 17-2*, U.S. SUP. CT., https://www.supremecourt.gov/search.aspx?filename=/docket/docketfiles/html/public/17-2.html [https://perma.cc/3YJA-PRTH] (last visited Feb. 14, 2018).

13. *Microsoft I*, 829 F.3d at 201.

14. *Id.* at 225 (Lynch, J., concurring) ("[T]he decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress.").

15. *See id.* at 221 (majority opinion) (noting that the government's reading of the SCA would allow "a United States judge [to] issue[] an order requiring a service provider to 'collect' from servers located overseas and 'import' into the United States data, *possibly belonging to a foreign citizen*, simply because the service provider has a base of operations within the United States" (emphasis added)); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *9 (D.N.J. July 10, 2017) ("[T]his Court concludes that compelling Google to provide all responsive information to the search warrant issued in this matter, regardless of whether the information is stored on computer servers outside of the United States, does not violate the presumption against extraterritorial application of United States law."); Jennifer Daskal, *There's No Good Decision in the Next Big Data Privacy Case*, N.Y. TIMES (Oct. 18, 2017), https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacy-court.html [https://perma.cc/H8K6-R8PH].

16. *See In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *26 (D.D.C. July 31, 2017).

17. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 724 (E.D. Pa.) (describing concerns about providers either storing data in countries that will not cooperate with U.S. law enforcement requests or using networks which move data throughout the world unpredictably), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

18. *See Microsoft I*, 829 F.3d at 221.

19. *See infra* Part II.C.1.

20. *See infra* Part II.C.2.

21. *See, e.g.*, *Microsoft I*, 829 F.3d at 233 (Lynch, J., concurring) ("Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised . . . .").

Current legislation and existing legal doctrines leave courts with limited and unappealing options to sufficiently address this problem.[22] In addition, the legislature may be inherently better equipped to address this kind of issue, in part because courts may struggle to effectively resolve extraterritoriality questions due to constitutional uncertainty.[23] Although the Fourth Amendment may apply to the email contents of U.S. citizens,[24] the extent of Fourth Amendment protection for data stored abroad is less clear.[25] Without a modern, workable statute to apply, the judiciary's primary nonstatutory means of regulating government access to records—the Fourth Amendment—would apply inconsistently (or perhaps not at all) in these circumstances.[26] Therefore, the best solution to this issue likely ought not to originate in the courts but from the legislature instead.

The International Communications Privacy Act (ICPA) is a previously introduced bill that provides a good starting point for legislation in this area.[27] Building upon the ICPA and expanding on ideas introduced by scholars,[28] this Note proposes that new legislation should create two separate investigative instruments: (1) a warrant for U.S. citizens and those with sufficient U.S. contacts and (2) a probable cause order for nationals of foreign countries.[29] This structure would ensure sufficient safeguards based in comity, respect for the privacy laws of other nations, and cognizance of the position of providers who may be placed in the middle of a conflict-of-laws situation. Simultaneously, it would allow legitimate investigations of U.S. citizens and those located in the United States to move forward swiftly and efficiently. Law enforcement, service providers, customers, and courts would all benefit from the clarity of knowing when and how U.S. law

22. *See infra* Part I.B–C.

23. *See infra* Parts I.B.1, II.B.

24. *See* United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) ("[A] subscriber enjoys a reasonable expectation of privacy in the contents of emails 'that are stored with, or sent or received through, a commercial ISP.'" (quoting Warshak v. United States, 490 F.3d 455, 473 (6th Cir. 2007))); *see also infra* Part I.B.1.

25. *See infra* Part I.B.1.

26. *See infra* Part I.B.1.

27. International Communications Privacy Act, H.R. 3718, 115th Cong. (2017); International Communications Privacy Act, S. 1671, 115th Cong. (2017). At the time of this Note's publication, several lawmakers who had introduced the ICPA announced a revamped version of that legislation, the "Clarifying Lawful Overseas Use of Data Act" or "CLOUD Act." CLOUD Act, H.R. 4943, 115th Cong. (2018); CLOUD Act, S. 2383, 115th Cong. (2018); *see also* Press Release, Orrin G. Hatch, U.S. Senator, Hatch Previews CLOUD Act: Legislation to Solve the Problem of Cross-Border Data Requests (Feb. 5, 2018), 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/65YK-U8K9] (referring to the CLOUD Act as an "outgrowth" of the ICPA). While this Note does not discuss the new bill in depth, it notes some key differences between the ICPA and the CLOUD Act. *See infra* Part II.D. Likewise, the CLOUD Act is referenced in relation to this Note's proposed legislative solution. *See infra* Part III.

28. *See* Kerr, *supra* note 4, at 416–17 (recommending legislative change that accounts for user identity over data storage location); Daskal, *supra* note 15 (recommending the same).

29. This Note proposes a legislative framework that is not controlled by storage location. Thus, the two categories of subscribers addressed are citizens and permanent residents of the United States ("U.S. persons") and foreign citizens without those U.S. contacts.

enforcement can access the contents of electronic communications stored by providers.

Microsoft[30] highlights a major problem with the SCA: the law reaches the data of both citizens and noncitizens but fails to distinguish between subscribers who should be fully subject to the laws of the United States and those who fall under another government's protection. The best solutions to this problem will draw clear distinctions between those two groups.

Part I of this Note first describes the current technological and legal landscape of electronic searches and seizures, specifically those occurring abroad. Part I then discusses the Second Circuit's holding in *Microsoft I* as well as the reasoning of judges that have rejected *Microsoft I*. These cases highlight the difficulty of applying the SCA in a world of cloud technology and global data storage. Part II explores the limited options available to the Supreme Court to address the issues in *Microsoft*, discusses why a legislative solution is better than what the courts can offer, looks at the potential legislative interests of the major stakeholders, and examines a legislative solution in the form of the ICPA. Finally, Part III proposes a strategy, building upon the ICPA, that would explicitly differentiate between the data of United States and foreign customers of service providers who store data abroad.

I. BACKGROUND

Beginning with the relevant technological background, Part I.A discusses the structure of global cloud networks and the international trend of data localization laws. Parts I.B and I.C describe the current state of Fourth Amendment doctrine in the realm of electronic communications as it applies to both citizens and noncitizens, as well as the statutory protections provided by the SCA. Finally, Part I.D explores the difficulties of applying the SCA in this technological context beginning with the most prominent example, *Microsoft*, and proceeding to examine the cases that have declined to follow that decision.

A. The Current Technological Context: Cloud Storage and International Data Regulation

High-speed internet and abundant electronic storage allow people to store, use, and access electronic data in a manner that poses challenges to existing laws like the SCA. The rise of cloud computing and service providers' use

30. Throughout the text of this Note, *Microsoft* refers generally to the case that has been granted certiorari and will be decided by the U.S. Supreme Court. United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2). *Microsoft I* refers to the Second Circuit's holding in favor of Microsoft. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197 (2d Cir. 2016). *Microsoft II* refers to the Second Circuit's denial of the motion to rehear the case en banc. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53 (2d Cir. 2017).

of servers[31] throughout the world means that electronic information can be moved or reproduced across international borders almost instantaneously.[32] Service providers' capacity to move data in this manner, however, has led to data localization and privacy measures that restrict the international flow of data.[33]

1. The Cloud and Network Architecture

The Supreme Court has described cloud computing as "the capacity of Internet-connected devices to display data stored on remote servers rather than on the device itself."[34] The National Institute of Standards and Technology defines cloud computing, perhaps more precisely, as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[35]

Cloud computing is the technology that allows users of web-based email services (such as Google's Gmail, Microsoft's Outlook, and Yahoo Mail) to access and send communications from any device that can connect to the internet.[36] This technology works by storing a user's communications on the provider's servers and giving an end user on-demand access to the data.[37] These cloud-based email services are ubiquitous throughout much of the world: Google, for example, reported in early 2016 that Gmail had over one billion active worldwide users—more than doubling the roughly 425 million users the company reported in 2012.[38]

Where and how this massive amount of data is stored depends on how a service provider has structured its network.[39] Two varieties of network architecture are relevant to this Note. The first is what Professor Paul Schwartz has called the "Data Localization" model, in which a company stores data in one country or region.[40] Microsoft is one of the companies that

---

31. "A 'server' is 'a shared computer on a network that provides service to clients.'" *Microsoft I*, 829 F.3d at 202 n.2 (quoting HARRY NEWTON & STEVE SCHOEN, NEWTON'S TELECOM DICTIONARY 1084 (28th ed. 2014)).

32. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 366–67 (2015).

33. *See* Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677, 713–14 (2015).

34. Riley v. California, 134 S. Ct. 2473, 2491 (2014).

35. *See* PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS & TECH., SPECIAL PUBLICATION 800-145, THE NIST DEFINITION OF CLOUD COMPUTING § 2 (2011).

36. *See* Paul M. Schwartz, *Information Privacy in the Cloud*, 161 U. PA. L. REV. 1623, 1633 (2013); *see also* MELL & GRANCE, *supra* note 35, § 2 (using web-based email as an example of a type of cloud service model).

37. *See* MELL & GRANCE, *supra* note 35, § 2.

38. Frederic Lardinois, *Gmail Now Has More Than 1B Monthly Active Users*, TECHCRUNCH (Feb. 1, 2016), https://techcrunch.com/2016/02/01/gmail-now-has-more-than-1b-monthly-active-users/ [https://perma.cc/L3RP-J4FC].

39. *See* Paul M. Schwartz, Legal Access to Cloud Information: Data Shards, Data Localization, and Data Trusts 5–6 (July 24, 2017) (unpublished manuscript), https://ssrn.com/abstract=3008392 [https://perma.cc/X64Q-XRAX].

40. *Id.* (manuscript at 5).

use this type of data storage scheme.[41] The second type of cloud storage has been called the "Data Shard" model.[42] "Sharded" data is separated into pieces that can be stored in separate locations.[43] Partitioning data in this way has security benefits[44] and is said to optimize network performance and efficiency.[45] Sharding is used by Google for its cloud services, including Gmail.[46]

Localization and sharding are two examples of different approaches to cloud storage. However, providers using these approaches typically do not operate their networks in a uniform way that makes the location of data, or the provider's knowledge thereof, predictable. Professor Orin Kerr looked into the matter after the Second Circuit's holding in *Microsoft I* and found that

> [s]ome providers make a point of figuring out the country of origin of each user, and they try to store user emails in that country or region. Other providers don't. Some providers know in what country a particular user's email will be located, and that answer is reasonably stable over time. Other providers don't, and it isn't. Some providers can access email stored abroad from wherever it is located. Other providers can't.[47]

In short, though cloud networking strategies can be categorized generally, the specific operation of each provider's network can and does vary.[48]

2. Maintaining Local Control of Data: Data Localization and International Privacy Concerns

The volume of potentially sensitive cloud data stored throughout the world is an aspect of the global internet that may thwart governments' efforts to regulate and protect sensitive information pertaining to their citizens. The fact that many of these cloud providers are based in the United States and are subject to U.S. jurisdiction also drives these concerns.[49] Since Edward Snowden exposed the broad scope of U.S. intelligence operations and electronic surveillance, a number of countries have moved to pass laws that

41. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 202 (2d Cir. 2016) (explaining that Microsoft's cloud service is "segmented into regions, and most customer data (*e.g.* email . . .) is generally contained entirely within one or more data centers in the region in which the customer is located").

42. *See* Schwartz, *supra* note 39 (manuscript at 5).

43. Chander & Lê, *supra* note 33, at 719.

44. *See id.*

45. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 712 (E.D. Pa.), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

46. *See* Schwartz, *supra* note 39 (manuscript at 5).

47. 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/ [https://perma.cc/MFB2-PBV3].

48. *Id.*

49. *See* Chander & Lê, *supra* note 33, at 714.

would "localize" data.[50] These laws attempt to ensure that electronic records are only stored domestically, within reach of that government and that government alone.[51]

Some countries apply localization requirements to only certain kinds of data. For example, Australia's law applies to medical records that include personal identifying information.[52] Other countries apply data localization laws more broadly, regulating all providers who operate within their borders.[53] These governments justify their laws by citing international security concerns (specifically, foreign surveillance), citizens' privacy concerns, domestic security concerns (specifically, law enforcement's access to records), and domestic economic development.[54]

A major recent development in the European Union, driven by personal privacy concerns, is the European General Data Protection Regulation (GDPR).[55] Effective May 25, 2018, the GDPR sets out new obligations for businesses that handle personal data and delineates new rights for the individuals to whom the data pertains.[56] Under the GDPR, a "controller" or "processor"[57] of data may only comply with a demand for data from a non-EU court if the demand is "based on an international agreement" between the two nations.[58] If a company violates this directive, it may suffer economic penalties.[59]

The variations of this international trend reflect a common goal among governments to maintain control over access to electronic data pertaining to their citizens. To accomplish these goals, many governments employ a policy of keeping data physically within their borders and imposing penalties on those who remove it.

B. Judicial Privacy Protection: Constitutional Limits to Searches and Seizures Abroad and in the Cloud

The massive amount of data described in Part I.A is a potential evidentiary treasure trove for law enforcement. However, the Fourth Amendment protects "the people" from "unreasonable searches and seizures."[60] Third-party cloud storage raises questions about what constitutes a search or seizure

50. *Id.* ("Anger at disclosures of U.S. surveillance abroad has led some countries to respond by attempting to keep data from leaving their shores . . . .").

51. *See id.* at 679.

52. *Id.* at 683.

53. *See id.* at 682.

54. *Id.* at 713.

55. Regulation 2016/679, General Data Protection Regulation, 2016 O.J. (L 119) 1 (EU).

56. Matt Burgess, *What Is GDPR? WIRED Explains What You Need to Know*, WIRED (Jan. 12, 2018), http://www.wired.co.uk/article/what-is-gdpr-uk-eu-legislation-compliance-summary-fines-2018 [https://perma.cc/5MVV-8FMV].

57. The "controller" is the entity that makes decisions about what data is stored, and the "processor" is the entity that does the actual processing of data. *See* Regulation 2016/679, *supra* note 55, art. 4(7)–(8).

58. *See id.* art. 48.

59. *See id.* art. 83.

60. *See* U.S. CONST. amend. IV.

of electronic records held by a provider and, where providers have both U.S. and non-U.S. customers, who "the people" are.

This Part looks at the strain that electronic storage and cloud technology place on traditional doctrines of search and seizure and at the difficulty of determining what protection the constitution affords foreign citizens and records stored in foreign countries.

1. Warrants, the Fourth Amendment, and Global Data Storage

The history of the warrant as an investigative tool goes back to English common law, where a "general warrant" gave the holder "blanket authority" to perform a search that was not limited to a specific location.[61] The Fourth Amendment was drafted with language designed to eliminate the abuses of these general warrants.[62]

Warrants traditionally authorize the government to perform searches and seizures that the Fourth Amendment would otherwise prohibit.[63] Though many warrants authorize both a search and a seizure, the two are distinct.[64] A search infringes on an individual's objectively reasonable and societally recognized expectation of privacy.[65] Seizures, on the other hand, interfere with an individual's possessory interest in a meaningful way.[66]

The Supreme Court has not addressed whether the Fourth Amendment protects consumers' email and other electronic communications held by third parties.[67] The traditional "third-party doctrine" holds that individuals do not retain a reasonable expectation of privacy in information that has been disclosed to a third party.[68] Therefore, under the third-party doctrine, even an individual who discloses information in reliance on a third party's confidence loses Fourth Amendment protection with regard to the disclosed information.[69]

However, exceptions to the doctrine are emerging as major forms of communication, such as email and cell phones, increasingly require

61. Payton v. New York, 445 U.S. 573, 583–84 & n.21 (1980) (quoting Stanford v. Texas, 379 U.S. 476, 481 (1965)).

62. U.S. CONST. amend. IV ("[N]o Warrants shall issue, but upon probable cause . . . and *particularly describing the place to be searched* and the persons or things to be seized." (emphasis added)).

63. *See* Johnson v. United States, 333 U.S. 10, 13 (1948).

64. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

65. *Id.*; Katz v. United States, 389 U.S. 347, 361 (1967).

66. *Jacobsen*, 466 U.S. at 113.

67. *United States v. Carpenter* raises a potential challenge to the third-party doctrine in the context of cell phone records. *See* United States v. Carpenter, 819 F.3d 880, 888–89 (6th Cir. 2015), *cert. granted*, 137 S. Ct. 2211 (argued Nov. 29, 2017) (16-402). At the time of this Note's publication, the Court had not issued an opinion in this case.

68. *See, e.g.*, Smith v. Maryland, 442 U.S. 735, 743–44 (1979) ("This Court consistently has held that a person has no legitimate expectation of privacy in information he voluntarily turns over to third parties.").

69. *See* United States v. Miller, 425 U.S. 435, 443 (1976).

disclosure to a third party.[70] In *United States v. Warshak*,[71] the Sixth Circuit recognized that users have a reasonable expectation of privacy in the content of their emails and held that a warrantless search of those communications violated the Fourth Amendment.[72] Courts that have addressed this and similar questions after *Warshak* acknowledge that the Fourth Amendment protects email content based on a reasonable expectation of privacy.[73]

Where a Fourth Amendment "search" concerns an individual's privacy, a Fourth Amendment "seizure" concerns the government's meaningful interference with an individual's possessory interest in an object.[74] In the physical world, this is a simple concept: if the government facilitates the removal of a mobile home, for example, it has seized that mobile home.[75] But when the warrant targets electronic records that are to be copied but otherwise undisturbed, it is unclear what exactly constitutes a seizure.[76]

There is doctrinal ambiguity on the question whether electronically copying computer data should trigger the Fourth Amendment's protections.[77] In many cases, electronic documents may be instantaneously copied and transferred in a manner similar to someone photocopying,[78] photographing,[79] or writing down a serial number[80] from potential evidence—all cases in which courts have held that there was no meaningful interference with the owner's possessory interests and, thus, no Fourth Amendment seizure.[81] However, the relatively limitless nature of what can be electronically stored has caused courts in other cases to refer to large-scale copying of electronic data as a seizure.[82]

Rule 41 of the Federal Rules of Criminal Procedure does not clarify the matter. As to electronic records, it states that "[a] warrant under Rule 41(e)(2)(A) may authorize the seizure of electronic storage media or the *seizure or copying* of electronically stored information."[83] The rule fails to define the parameters of what constitutes a seizure with regard to

70. *See, e.g.*, *In re* U.S. for an Order Authorizing the Release of Historical Cell-Site Info., 809 F. Supp. 2d 113, 123 (E.D.N.Y. 2011) (discussing the "content exception" to the third-party doctrine).

71. 631 F.3d 266 (6th Cir. 2010).

72. *See id.* at 274.

73. *See, e.g.*, Coughlin v. Town of Arlington, No. 10-10203-MLW, 2011 WL 6370932, at *11 (D. Mass. Dec. 19, 2011); *In re U.S. for an Order Authorizing the Release of Historical Cell-Site Info.*, 809 F. Supp. 2d at 125.

74. *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).

75. *See* Soldal v. Cook County, 506 U.S. 56, 61 (1992).

76. *See* Orin S. Kerr, *Fourth Amendment Seizures of Computer Data*, 119 YALE L. J. 700, 703 (2010) ("Whether and when copying [data] amounts to a seizure remains an unsolved puzzle.").

77. *See id.*

78. *See* United States v. Thomas, 613 F.2d 787, 793 (10th Cir. 1980).

79. *See* United States v. Mancari, 463 F.3d 590, 596 (7th Cir. 2006).

80. *See* Arizona v. Hicks, 480 U.S. 321, 324 (1987).

81. *See id.*; *Mancari*, 463 F.3d at 596; *Thomas*, 613 F.2d at 793.

82. *See* United States v. Ganias, 755 F.3d 125, 135–36 (2d Cir. 2014) (describing mirroring a hard drive as a Fourth Amendment seizure); United States v. Comprehensive Drug Testing, 621 F.3d 1162, 1172 (9th Cir. 2010) (per curiam) (referring to electronically copied files as "seized" pursuant to a warrant).

83. FED. R. CRIM. P. 41(e)(2)(B) (emphasis added).

electronically stored data and may imply that the two are different because it mentions copying as distinct from seizure.[84]

Courts generally assume that a warrant unilaterally issued by a judge in the United States is only effective within this country.[85] In the context of traditional search warrants, which require police presence during the search, "courts *may not* issue warrants for extraterritorial searches."[86] The typical understanding of a warrant's reach is that "[t]he domestic warrant authority, whether construed under Rule 41, the common law, or a statutory authority, does not ordinarily extend to the property of foreigners abroad."[87]

Like the authority to issue warrants, the application of the Fourth Amendment is not universal.[88] In determining whether the Fourth Amendment applies to a search, the Supreme Court has looked at whether the search or seizure occurs within the United States or abroad as well as the identity and contacts of the individual invoking the right.[89] Searches inside the United States, for example, even of a non-U.S. citizen, are governed by the Fourth Amendment.[90] Additionally, U.S. citizens retain some Fourth Amendment rights when outside the United States.[91] In contrast to the probable cause standard that applies within the United States, however, circuit courts have required mere "reasonableness" for searches of U.S. citizens abroad.[92] As a result, the full warrant and probable cause requirements end at the border, even for U.S. citizens. The reasonableness test that has been applied in the Second and Seventh Circuits balances the

84. *See* Mark Taticchi, Note, *Redefining Possessory Interests: Perfect Copies of Information as Fourth Amendment Seizures*, 78 GEO. WASH. L. REV. 476, 489–90 (2010).

85. *See* United States v. Verdugo-Urquidez, 494 U.S. 259, 274 (1990) (noting that a warrant would be a "dead letter outside the United States"); United States v. Stokes, 726 F.3d 880, 892–93 (7th Cir. 2013); United States v. Odeh (*In re* Terrorist Bombings of U.S. Embassies in E. Afr.), 552 F.3d 157, 171 (2d Cir. 2008) ("[I]f U.S. judicial officers were to issue search warrants intended to have extraterritorial effect, such warrants would have dubious legal significance, if any, in a foreign nation."); *see also* FED. R. CRIM. P. 41(b)(5)(A) (providing that warrants may issue for property "outside the jurisdiction of any state or district, but within . . . a United States territory, possession, or commonwealth").

86. *In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *15 (D.D.C. July 31, 2017) (emphasis added).

87. Orin Kerr, *Microsoft Challenged the Wrong Law. Now What?*, LAWFARE (Nov. 27, 2017, 11:00 AM), https://www.lawfareblog.com/microsoft-challenged-wrong-law-now-what [https://perma.cc/SNN9-D48W].

88. *See Verdugo-Urquidez*, 494 U.S. at 274–75.

89. *See id.*

90. *See* Zadvydas v. Davis, 533 U.S. 678, 693 (2001) ("[T]he Due Process Clause applies to all 'persons' within the United States, including aliens, whether their presence here is lawful, unlawful, temporary, or permanent."); Daskal, *supra* note 32, at 340 ("If [a search or seizure takes place] in the United States, the Fourth Amendment applies.").

91. *See Verdugo-Urquidez*, 494 U.S. at 270.

92. *See* United States v. Odeh (*In re* Terrorist Bombings of U.S. Embassies in E. Afr.), 552 F.3d 157, 171 (2d Cir. 2008) ("[T]he Fourth Amendment's Warrant Clause has no extraterritorial application and . . . foreign searches of U.S. citizens conducted by U.S. agents are subject only to the Fourth Amendment's requirement of reasonableness."); *see also* United States v. Stokes, 726 F.3d 880, 885 (7th Cir. 2013).

severity of the privacy invasion against the government's justification for the search.[93]

For searches of property located outside the United States, the owner of the property must have sufficient voluntary contacts with the United States to invoke the Fourth Amendment.[94] Where courts find a noncitizen's voluntary contacts with the United States insufficient, the Fourth Amendment simply does not protect that person.[95] In the modern age, it is unclear whether voluntary contact with the United States *online* would similarly establish Fourth Amendment rights.[96]

Thus, current Fourth Amendment doctrine is unsettled with regard to the copying of electronic records held by a service provider (as a third party) and the constitutional protections granted to records stored abroad.

2. Subpoenas and Extraterritoriality

Though warrants generally do not reach records stored abroad, subpoenas often do.[97] Where full Fourth Amendment or statutory protections requiring a warrant are nonexistent or ill defined—as is the case with electronic records stored abroad by third parties—subpoenas take on additional importance for government access to records.[98]

In many cases, the government can use a subpoena to compel the production of evidence in an investigation.[99] Grand jury subpoenas are issued in criminal investigations without judicial input,[100] and they are presumptively enforceable unless the recipient can show that compliance would somehow be unreasonable.[101] In criminal investigations, a subpoena

---

93. *See Stokes*, 726 F.3d at 893; *In re Terrorist Bombings*, 552 F.3d at 172.

94. *See Verdugo-Urquidez*, 494 U.S. at 271–73.

95. *See* United States v. Emmanuel, 565 F.3d 1324, 1331 (11th Cir. 2009) ("[T]he Fourth Amendment does not apply to nonresident aliens whose property is searched in a foreign country . . . ."). For an in-depth discussion of what voluntary contacts courts have found sufficient or insufficient to establish Fourth Amendment rights, see Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 293–94 (2015).

96. *See* Kerr, *supra* note 95, at 304–05 (arguing that purely online contact with the United States should not be sufficient for establishing Fourth Amendment rights).

97. *See* Marc Rich & Co. v. United States, 707 F.2d. 663, 667 (2d Cir. 1983) (noting that a witness many not "resist the production of documents on the ground that the documents are located abroad"); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(a) (AM. LAW INST. 1987) ("A court or agency in the United States, when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the United States."); *see also* United States v. Bank of N.S., 740 F.2d 817, 828 (11th Cir. 1984).

98. *See* Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST (July 7, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/?utm_term=.274bc6a00896 [https://perma.cc/FV5W-VL5G].

99. *See* FED. R. CRIM. P. 17(c)(1) ("A subpoena may order the witness to produce any books, papers, documents, data, or other objects the subpoena designates.").

100. *See id.* r. 17(a) (providing that federal subpoenas with the clerk's signature and seal should be given to the requesting party to fill out and serve).

101. *See* United States v. R. Enters., Inc., 498 U.S. 292, 301 (1991) ("[A] grand jury subpoena issued through normal channels is presumed to be reasonable, and the burden of

can compel the production of documents held abroad only if the recipient of that subpoena is subject to the court's jurisdiction.[102] The storage location of the subpoenaed documents is irrelevant[103]: if a company has the power to move the records from one location to another, production is required unless a court finds that request is unreasonable.[104] Inconsistent legal obligations based on the storage of records abroad may provide a ground to object to a subpoena, but a court may still choose to order a party to produce records even if it risks penalties for doing so abroad.[105]

When a party challenges a subpoena based on extraterritoriality, the court will engage in a comity analysis.[106] The factors to be balanced in a comity analysis include the importance of the documents to the investigation, how narrow and specific the request is, where the record originated, alternative options for obtaining the record, and the relative interests of the United States and the foreign state.[107] Further, courts are more likely to command parties to produce their own records than records held on behalf of a third party or customer.[108]

As demonstrated above, the absence of Fourth Amendment or statutory privacy protections allow subpoenas to reach records stored beyond the borders of the United States, limited in most cases only by a general comity analysis.[109] For electronic records that are unevenly protected by the Fourth Amendment, the statutory protections discussed in Part I.C provide a second layer of privacy protection.

C. Statutory Privacy Protection: The Stored Communications Act

While courts possess general mechanisms like the Fourth Amendment and the doctrine of comity to protect privacy, legislatures in the United States regularly enact more specific statutory protections. Often, these statutes are designed to provide protection in areas where the judiciary has not, or is not,

showing unreasonableness must be on the recipient who seeks to avoid compliance."); *see also* FED. R. CRIM. P. 17(c)(2) ("On motion made promptly, the court may quash or modify the subpoena *if compliance would be unreasonable or oppressive*." (emphasis added)).

102. *See Marc Rich & Co.*, 707 F.2d at 667; RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 cmt. b.

103. *See Marc Rich & Co.*, 707 F.2d at 667 ("The test for the production of documents is control, not location.").

104. *See* United States v. First Nat'l City Bank, 396 F.2d 897, 901–02 (2d Cir. 1968); *see also* FED. R. CRIM. P. 17(c)(2).

105. *See* United States v. Bank of N.S., 740 F.2d 817, 826–29 (11th Cir. 1984).

106. *See* Société Nationale Industrielle Aérospatiale v. U.S. Dist. Court for S. Dist. of Iowa, 482 U.S. 522, 543–44 (1987); Richmark Corp. v. Timber Falling Consultants, 959 F.2d 1468, 1474–78 (9th Cir. 1992) (balancing China's interests in enforcing a law that prohibited disclosure of documents sought in discovery against the United States' interest in obtaining the information); *Bank of N.S.*, 740 F.2d at 826–29; RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c).

107. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c).

108. *See* Schwartz, *supra* note 39 (manuscript at 20).

109. *See* Marc Rich & Co. v. United States, 707 F.2d. 663, 667 (2d Cir. 1983); RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442(1)(c); Kerr, *supra* note 98.

expected to provide protection.[110] This Part explores the federal law[111] that both protects and provides access to electronic data. First, this Part explains the origins of the SCA, then it describes in greater detail what the warrant provision of the SCA does and how some important amendments have altered it.

1. A Brief History of the SCA

The SCA,[112] enacted as Title II of the ECPA,[113] creates privacy rights for certain types of electronic communications.[114] The statute also provides procedures for law enforcement to compel disclosure of those records.[115] Congress passed the SCA to provide statutory protection for electronic records that were not clearly protected by the Fourth Amendment.[116]

The SCA protects the records of individuals using electronic communications services (ECS) and remote computing services (RCS).[117] The distinction between these two was meaningful in 1986: "[t]he ECS protections covered email; the RCS protections covered contents of communications transmitted for remote storage and processing by services available to the public."[118] Today, the distinction raises "complex and perhaps unanswerable questions" about how the law applies to providers and services that are often multifunctional and might be classified as both ECS and RCS.[119]

Section 2703 of the SCA sets procedures for government access to the electronic records that § 2702 protects.[120] While different classes of records receive different levels of protection, the procedures necessary for acquiring more-protected records also cover less-protected records (i.e., a warrant may authorize the government to obtain any records that a subpoena could be used

110. *See* Orin S. Kerr, *The Effect of Legislation on Fourth Amendment Protection*, 115 MICH. L. REV. 1117, 1140 (2017) ("Legislatures usually pass privacy laws when it seems necessary because legislators expect the courts to stay out.").

111. This Note focuses on federal law enforcement's power under the ECPA and SCA, and thus foreign surveillance and data collection under the Foreign Intelligence Surveillance Act (FISA) is outside of its scope. For a discussion of how FISA and related authorities treat territoriality, see Daskal, *supra* note 32, at 343–54.

112. 18 U.S.C. §§ 2701–2712 (2012).

113. *See* Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C.).

114. *See* 18 U.S.C. § 2702; *see also* Kerr, *supra* note 4, at 383.

115. *See* 18 U.S.C. § 2703; *see also* Kerr, *supra* note 4, at 383–84.

116. *See* Kerr, *supra* note 4, at 376–77 ("The original ECPA was designed as a statutory stand-in for uncertain Fourth Amendment protection.").

117. 18 U.S.C. § 2702.

118. *See* Kerr, *supra* note 4, at 395. For example, a commercial email provider might be classified as an ECS when it stores the unopened email of a subscriber but as an RCS after the email is opened and stored on the provider's servers. *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, 1216 (2004).

119. *See* Kerr, *supra* note 4, at 397; *see also* Alexander Scolnik, Note, *Protections for Electronic Communications: The Stored Communications Act and the Fourth Amendment*, 78 FORDHAM L. REV. 349, 382–83 (2009).

120. *See* 18 U.S.C. § 2703.

to obtain).[121] With exceptions, the statute requires law enforcement to obtain a warrant to compel a provider to release contents of communications.[122] Section 2703 also creates a court order[123] and allows for the release of noncontent name, address, and other records by subpoena.[124]

2. The SCA's Warrant Provision

The warrant provision[125] of the SCA provides that the government may require a service provider to disclose the contents of certain electronic communications "pursuant to a warrant issued using the procedures described in the Federal Rules of Criminal Procedure (or, in the case of a State court, issued using State warrant procedures)."[126] On its face, the SCA requires a warrant for emails in "electronic storage" with an ECS for fewer than 180 days[127] and for records stored with an RCS in lieu of providing notice to the subscriber.[128] However, it has been the DOJ's practice since 2013 to obtain warrants for all email content that it seeks in criminal cases.[129]

Warrants under the SCA are issued "using the procedures described in the Federal Rules of Criminal Procedure"[130]—specifically, Rule 41.[131] Rule 41 codifies the constitutional requirement that law enforcement must establish probable cause to obtain a warrant[132] and sets limits on a court's jurisdiction that are typically based on the location of the person or property targeted by the warrant.[133] Prior to the SCA's amendment in 2001, Rule 41 limited a court's jurisdiction under the statute to issue a warrant to persons or property located within that court's district[134] or for property outside that district if it related to a crime that occurred within the issuing district.[135]

---

121. *See id.* § 2703(c).
122. *Id.* § 2703(a)–(b)(1)(A).
123. *Id.* § 2703(d).
124. *Id.* § 2703(c)(2).
125. *Id.* § 2703(a)–(b)(1)(A).
126. *Id.*
127. *Id.* § 2703(a).
128. *Id.* § 2703(b)(1).
129. *See* H.R. REP. NO. 114-528, at 9 (2016) ("Soon after [*United States v. Warshak*], the Department of Justice began using warrants for email in all criminal cases. That practice became Department policy in 2013."); *see also* Statement, Richard Salgado, Director, Law Enf't & Info. Sec., Google Inc., Hearing Before the House Committee on the Judiciary, Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era (June 15, 2017) (unpublished testimony), http://docs.house.gov/meetings/JU/JU00/20170615/106117/HHRG-115-JU00-Wstate-SalgadoR-20170615.pdf [https://perma.cc/32GZ-MYCN] ("[A] warrant-for-content standard is effectively the law of the land today. This standard is observed by governmental entities and providers alike . . . .").
130. 18 U.S.C. § 2703(a)–(b)(1)(A).
131. FED. R. CRIM. P. 41.
132. *Id.* r. 41(d) ("After receiving an affidavit or other information, a magistrate judge . . . must issue the warrant if there is probable cause to search for . . . property . . . .").
133. *See id.* r. 41(b).
134. *See id.* r. 41(b)(1).
135. *See id.* r. 41(b)(5). Warrants issued under Rule 41(b)(5) are limited to property that can be found either in a U.S. territory, possession, or commonwealth, or on property abroad that has some connection to U.S. diplomatic or consular missions. *See id.* r. 41(b)(5)(A)–(C).

In the wake of September 11, 2001, Congress amended the SCA's warrant provision in two key ways. First, it expanded a court's jurisdiction to issue SCA warrants beyond the standard limits of Rule 41—jurisdiction to issue an SCA warrant may be premised solely on the issuing court's jurisdiction over the crime the government is investigating.[136] This amendment "expand[s] a court's authority to issue a warrant [under the SCA] beyond Rule 41."[137]

Second, Congress changed the language of § 2703 from "issued under the Federal Rules of Criminal Procedure" to "issued *using the procedures* described in the Federal Rules of Criminal Procedure."[138] At least one judge characterized the change as an expression of congressional intent that SCA warrants be bound by "some—but not all—of the requirements of Rule 41."[139] Legislative history addressing this change indicates a concern about jurisdictional issues caused by the fact that a judge in the district where the service provider was located had to issue the warrant.[140] The 2001 amendments move the SCA away from Rule 41 in some key respects—but how far away is unclear and has been a point of disagreement among courts interpreting the SCA.[141]

D. What's Extraterritorial When It Comes to the SCA?: Microsoft I *and Its Rebellious Progeny*

As the previous Parts explain, the SCA regulates the government's access to data stored by service providers that use global storage networks. With regard to content records, this raises an issue as to whether compelling the retrieval and production of records stored abroad constitutes an extraterritorial extension of the SCA warrant. This Part explores how courts have interpreted the SCA in light of this issue.

First, Part I.D.1 explores the legal rationales for the Second Circuit's holding in *Microsoft I* that data stored abroad are out of the reach of an SCA

136. *See* 18 U.S.C. § 2711(3)(A) (2012) (providing that warrants under the SCA can be issued by "any district court of the United States . . . or any United States court of appeals that . . . has jurisdiction over the offense being investigated"); *see also In re* Search Warrant to Google, Inc., No. MAG 16-4116, 2017 WL 2985391, at *8 (D.N.J. July 10, 2017) (discussing this amendment to the SCA).

137. *In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *8.

138. 18 U.S.C. § 2703 (emphasis added).

139. *In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *21 (D.D.C. July 31, 2017).

140. *See* H.R. REP. NO. 107-236, at 57 (2001) (introducing the SCA amendment as permitting "nationwide" service of warrants to avoid a situation where investigators looking for emails related to a crime in their own city must enlist investigators in another state simply because the service provider is located there).

141. *Compare* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 213 (2d Cir. 2016) ("Although some [amendments] address the reach of SCA warrants, none of the amendments contradicts the term's traditional domestic limits."), *with In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *21 n.24 ("[W]hile § 2703 incorporates more than just the probable cause requirement of Rule 41, the territorial limitations of Rule 41 are not among the Rule 41 'procedures' applied to SCA warrants.").

warrant. Part I.D.2 then looks at the strong dissenting opinions from the Second Circuit's denial of rehearing en banc,[142] as well as a series of district court opinions rejecting Google's use of the *Microsoft I* precedent to deny certain requests under the SCA.

1. *Microsoft I*

In *Microsoft I*, the U.S. government suspected that a customer's emails contained evidence of drug trafficking and served Microsoft with an SCA warrant commanding production of the emails.[143] Microsoft produced some noncontent records but moved to quash the warrant on the ground that the content was stored on servers located outside the territorial reach of the SCA warrant in Ireland.[144] The court analyzed the request based on the data storage location.[145] The nationality of the subscriber targeted by the investigation was undisclosed.[146]

The court's decision hinged on whether the use of an SCA warrant to retrieve records stored abroad violates the presumption against extraterritoriality, a canon of construction that assumes federal statutes are "'meant to apply only within the territorial jurisdiction of the United States,' unless a contrary intent clearly appears."[147] *Morrison v. National Australia Bank Ltd.*[148] and *RJR Nabisco, Inc. v. European Community*[149] set forth a two-part approach to analyze these cases. First, the court determines whether the provision of the statute explicitly permits extraterritorial application.[150] If the statute is not explicit in this regard, the court still must determine whether the "application" of the statute—here, using the warrant to compel Microsoft to bring records stored abroad into the United States to produce to law enforcement—is extraterritorial.[151] This second-stage determination examines the request in light of the "'territorial events or relationships' that are the 'focus' of the relevant statutory provision."[152]

The Second Circuit held that the statute does not provide for extraterritorial application of SCA warrants and that the application of the warrant to obtain records stored in Ireland under the control a U.S. entity *did* constitute an

142. *See generally* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53 (2d Cir. 2017) (denying rehearing en banc).

143. *Microsoft I*, 829 F.3d at 200.

144. *Id.* at 200–01.

145. *Id.* at 201 (framing the issue as whether a warrant can "require a service provider to retrieve material from beyond the borders of the United States").

146. *Id.* at 230 (Lynch, J., concurring) ("Because Microsoft relies solely on customers' self-reporting in classifying customers by residence, and [generally] stores emails . . . on local servers—and because the government did not include in its warrant application such information . . . we do not know the nationality of the customer.").

147. *Id.* at 210 (majority opinion) (quoting Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).

148. 561 U.S. 247 (2010).

149. 136 S. Ct. 2090 (2016).

150. *Microsoft I*, 829 F.3d at 210.

151. *Id.*

152. *Id.* at 216 (quoting Mastafa v. Chevron Corp., 770 F.3d 170, 183 (2d Cir. 2014)).

extraterritorial application of the warrant provision.[153] Federal law enforcement, therefore, could not use the warrant authority under the SCA to obtain the records; it would instead have to request the information from the Irish government through a Mutual Legal Assistance Treaty (MLAT).[154]

Though the case was decided on statutory rather than constitutional grounds, the court referenced the traditional limits of the Fourth Amendment and warrants at both stages of the extraterritoriality analysis. In discussing the textual limits of the SCA, the court stressed that Congress used "warrant" as a "term of art" in the SCA, which limits the statutory instrument in the same ways traditional search warrants are limited.[155]

Turning to the second prong of the *Morrison* analysis, the court determined that the SCA's focus is privacy.[156] The court based this conclusion on the statute's textual ties to the Federal Rules of Criminal Procedure[157] and Congress's intent to extend Fourth Amendment protections to electronic communications.[158] The court concluded that the warrant was applied extraterritorially because the SCA protects privacy where the data is accessed (i.e., its storage location).[159]

Further explaining the Fourth Amendment reasoning for its holding, the court opined that executing an SCA warrant turns the recipient entity into an agent of the government.[160] The result of this agency relationship is that "the Fourth Amendment's warrant clause applies in full force to the private party's actions."[161] Thus, the act of accessing the information at its stored location outside the United States is the act of a government agent rather than an independent service provider.[162] The court noted that this kind of compelled cooperation with a search is not unique to the SCA and does not

153. *Id.* at 222.

154. *Id.* at 221. MLATs "allow signatory states to request one another's assistance with ongoing criminal investigations, including issuance and execution of search warrants." *Id.* The MLAT process is considered an unappealing solution for law enforcement due to the long wait time for compliance and the fact that the United States does not even have these treaties with many countries. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 714 (E.D. Pa.), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017); Schwartz, *supra* note 39 (manuscript at 17).

155. *Microsoft I*, 829 F.3d at 212–13 ("Congress intended to invoke the term 'warrant' with all of its traditional, domestic connotations.").

156. *Id.* at 220.

157. *Id.* at 218 (noting that the statute adopts Rule 41 of the Federal Rules of Criminal Procedure and that Rule 41 "reflects the historical understanding of a warrant as an instrument protective of the citizenry's privacy").

158. *Id.* at 219–20.

159. *Id.* at 220 ("Having . . . determined that the [SCA] focuses on user privacy, we have little trouble concluding that execution of the Warrant would constitute an unlawful extraterritorial application of the [SCA].").

160. *See id.* at 214 ("When the government compels a private party to assist it in conducting a search or seizure, the private party becomes an agent of the government . . . .").

161. *Id.*

162. *See id.*

remove the SCA warrant from the territorial restrictions associated with warrants.[163]

The *Microsoft I* court also rejected the notion that an SCA warrant is a warrant-subpoena "hybrid" that takes on the extraterritorial properties of a subpoena.[164] The court found no textual or contextual support for this view in the statute[165] and rejected the idea that "Congress intended to jettison the centuries of law requiring the issuance and performance of warrants in specified, domestic locations, or to replace the traditional warrant with a novel instrument of international application."[166]

Moreover, the court distinguished the email content at issue from a party's own records[167] and banking records in which depositors do not have a protectable interest.[168] In *Microsoft I*, the records were different because Microsoft was "merely a caretaker for another individual or entity" who had a "protectable privacy interest" in the emails.[169] Despite some superficial similarities in the process of compliance with the instrument, the court found that SCA warrants are wholly distinct from subpoenas.[170]

The Second Circuit concluded that SCA warrants cannot be used to compel service providers to produce email content stored outside the United States.[171] This strict limit on SCA warrants provoked backlash both within the Second Circuit and in district courts throughout the country, as other providers (primarily Google) began invoking the decision to deny requests for records that previously would have been released.[172]

2. *Microsoft II* Dissents and the District Courts

In *Microsoft II*, the Second Circuit denied the government's motion to rehear the case en banc by a four-to-four plurality.[173] All four dissenting judges wrote separate opinions expressing their disagreement with both the legal conclusions in and the policy ramifications of *Microsoft I*.[174]

---

163. *See id.* ("[T]he law of warrants has long contemplated that a private party may be required to participate in the lawful search or seizure of items belonging to the target of an investigation.").

164. *Id.*

165. *Id.* ("[T]he SCA recognizes the distinction [between warrants and subpoenas] and, unsurprisingly, uses the 'warrant' requirement to signal (and to provide) a greater level of protection to priority stored communications . . . .").

166. *Id.* at 214–15.

167. *See id.* at 215.

168. *Id.* at 216 (citing United States v. Miller, 425 U.S. 435, 440–41 (1976)).

169. *Id.* at 215.

170. *Id.* at 214–15.

171. *Id.* at 222.

172. *See In re* Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, No. 2:16-mj-02197-DUTY-1, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 2017) ("Before the *Microsoft I* ruling, Google routinely responded to SCA warrants by querying its global network, foreign and domestic."); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *1 (D.N.J. July 10, 2017); Kerr, *supra* note 47.

173. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53, 54 (2d Cir. 2017).

174. *See id.* at 60 (Jacobs, J., dissenting); *id.* at 62 (Cabranes, J., dissenting); *id.* at 69 (Raggi, J., dissenting); *id.* at 74 (Droney, J., dissenting).

Following the dissenting judges in *Microsoft II*, every district court that has ruled on this issue has held that the application of an SCA warrant to obtain records[175] stored by a provider abroad is permissible.[176] Judges have articulated some distinct but often overlapping legal reasons for declining to follow *Microsoft I*. First, the warrant-subpoena hybrid view would hold that the effect of the SCA's warrant provision—what it permits the government to do and what it requires of service providers—should control rather than the legislature's choice of words.[177] Second, the Fourth Amendment-based rationale concludes that, when law enforcement officers execute an SCA warrant, they do not "seize" the records when they are stored abroad but merely search the records once they have been brought within the United States.[178] Third, the district courts in which Google has raised objections pursuant to *Microsoft I* have distinguished its holding based on the network design of each provider.[179] These lines of reasoning are addressed in turn.

a. Warrant-Subpoena Hybrid View

The first dissenting opinion in *Microsoft II*, written by Judge Dennis G. Jacobs, notes parenthetically that an SCA warrant "functions as a subpoena though the Act calls it a warrant."[180] Most of the judges who have disagreed with *Microsoft I* discuss this view, and it was central to the district court opinion that *Microsoft I* reversed.[181] These judges distinguish SCA warrants

175. There is some disagreement among these judges on the result under the first prong of the *Morrison* test. *Compare In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *9 ("The Court concludes that a plain reading of the SCA reveals it does not contain a clear expression of Congressional intent of extraterritorial application."), *with In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *15 (D.D.C. July 31, 2017) ("In the SCA, Congress authorized the government to use an SCA warrant, a subpoena, or a § 2703(d) order to compel defined types of service providers subject to the jurisdiction of U.S. courts to disclose electronic records under its control, *including such records stored abroad* . . . ." (emphasis added)).

176. *See In re* Search Warrant Issued to Google, Inc., 264 F. Supp. 3d 1268, 1278 (N.D. Ala. 2017); *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263-RS, 2017 WL 3478809, at *4 (N.D. Cal. Aug. 14, 2017); *In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *1; *In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com*, 2017 WL 3263351, at *8; *In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *1; *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 721 (E.D. Pa.), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

177. *See, e.g.*, *Microsoft II*, 855 F.3d at 60–62 (Jacobs, J., dissenting).

178. *See, e.g.*, *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d at 721.

179. *See supra* Part I.A.1.

180. *Microsoft II*, 855 F.3d at 60.

181. *See In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 471 (S.D.N.Y. 2014) ("[T]he [SCA warrant] is a hybrid: part search warrant and part subpoena. It is obtained like a search warrant . . . . On the other hand, it is executed like a subpoena . . . ."), *rev'd sub nom.* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

from traditional warrants based on the subpoena-like manner of the SCA warrant's execution.[182]

Under this view, an SCA warrant is simply "the procedural mechanism by which the government may require a service provider to disclose the contents of electronic communications."[183] The instrument is called a warrant but is bound by the procedures of Rule 41 only as far as probable cause is concerned.[184] An SCA warrant is not bound by the territorial concerns of warrants because it operates by requiring disclosure as opposed to authorizing government entry and seizure of materials from some premises.[185]

The cases distinguish SCA warrants from traditional search warrants, which "authorize government action as to *places*," because SCA warrants "authorize government action on *persons*."[186] SCA warrants, unmoored from the traditional territorial limits of search warrants, focus on the company that controls and can produce the records rather than on the place where the records are stored.[187] If the company is within the court's jurisdiction and has the ability to bring the records within the jurisdiction, then the application of the statute is not extraterritorial.[188]

b. Fourth Amendment Search-but-Not-Seizure View

The incongruity of the term warrant (with its territorial and Fourth Amendment implications) in the SCA and the reality that the service provider and not the government is the only party making (electronic) contact with anything outside the United States when warrants are executed lead some judges to adopt the "search-but-not-seizure" view.[189] The simplest statement of this argument comes from Judge José A. Cabranes's observation that the only part of Microsoft's conduct that would have been unlawful under the SCA, had there been no warrant, was giving the customer's records to the government.[190] While there is a statutory—and perhaps even a

182. *See, e.g.*, *In re* Search Warrant No. 16-960-M-1 to Google, No. 16-1061, 2017 WL 3535037, at *7 (E.D. Pa. Aug. 17, 2017).

183. *Id.*

184. *See In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *17 (D.D.C. July 31, 2017).

185. *See In re Search Warrant No. 16-960-M-1 to Google*, 2017 WL 3535037, at *7.

186. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53, 65 n.19 (2d Cir. 2017) (Cabranes, J., dissenting).

187. *Id.* at 70 (Raggi, J., dissenting).

188. *Id.* at 71; *see also id.* at 61 (Jacobs, J., dissenting) ("Extraterritoriality need not be fussed over when the information sought is already within the grasp of a domestic entity served with a warrant. The warrant in this case can reach what it seeks because the warrant was served on Microsoft, and Microsoft has access to the information sought.").

189. *See In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *9 (D.N.J. July 10, 2017) (holding that an SCA warrant "calls for a search and not a seizure").

190. *Microsoft II*, 855 F.3d at 68 (Cabranes, J., dissenting) ("Microsoft did not need a warrant to take possession of the emails stored in Ireland. Nor did it need a warrant to move

constitutional—privacy interest in stored electronic communications under this view, that privacy interest is not infringed (and thus, the protections of a warrant do not apply) until the records are handed off to the government.[191]

This argument is distinct from the argument that an SCA warrant is not a traditional warrant, though the two are not mutually exclusive.[192] They both lead to the same conclusion: obtaining records stored on foreign servers does not constitute an extraterritorial application of the SCA.[193] However, this view is less about distinguishing SCA warrants from traditional warrants and is more focused on how Fourth Amendment doctrine applies to cases where the government is passive throughout much of the process.[194]

The crux of this position is that nothing Microsoft or Google does in moving data around—even though they are doing so in order to comply with the government's demands—constitutes a Fourth Amendment "seizure" or "search."[195] When an SCA warrant is executed, the Fourth Amendment (and thus the warrant requirement) is only triggered when the provider turns the records over to the government for inspection.[196] That "search" by the government, once it has the records in hand, occurs domestically.[197] The fact that "the warrant calls for a search and not a seizure" satisfies the second prong of the *Morrison* test because "the conduct relevant to the extraterritorial analysis—*i.e.*, the location of the search—occurs entirely in the United States."[198]

For the most part, the courts that articulate this argument express the view that "[e]lectronically transferring data from a server in a foreign country to Google's data center in California does not amount to a 'seizure' because there is no meaningful interference with the account holder's possessory interest in the user data."[199] Some judges that extend this reasoning go on to

---

the emails from Ireland to the United States. It already had possession of, and lawful *access* to, the targeted emails from its office.").

191. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 721 (E.D. Pa.) ("When Google produces the electronic data in accordance with the search warrants and the Government views it, the actual invasion of the account holders' privacy—the searches—will occur in the United States."), *aff'd*, No. 16-1061, 2017 WL 3535037 (E.D. Pa. Aug. 17, 2017).

192. A number of courts, in reasoning through their rejection of the *Microsoft I* holding, have articulated both arguments. *See, e.g.*, *In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *15–22 (D.D.C. July 31, 2017).

193. *See In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *9; *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d at 722.

194. *See In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *9.

195. *See In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *10 (D.D.C. June 2, 2017), *aff'd*, No. 16-mj-00757 (BAH), 2017 WL 3445634 (D.D.C. July 31, 2017).

196. *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d at 721–22.

197. *Id.* (holding that the account holder's privacy is not invaded until the government searches the records, and "the actual invasion of the account holders' privacy—the searches—will occur in the United States").

198. *In re Search Warrant to Google, Inc.*, 2017 WL 2985391, at *9.

199. *In re Search Warrant No. 16-960-M-01 to Google*, 232 F. Supp. 3d at 720; *see supra* Part I.B.1.

explain why the service provider is not acting as an agent of the government when it transfers data.[200] Because the service providers in these cases already had lawful possession of the records in question, they cannot be said to have acted as a government agent to "seize" anything.[201]

c. Distinguishing the Google Cases from Microsoft I *on the Facts*

An important nuance to the discussion above is the difference between the facts of *Microsoft* and the Google cases in which judges have declined to extend *Microsoft I*. The data at issue in *Microsoft*, on the one hand, is apparently all stored on a server in Ireland.[202] There are indications in the record that the target subscriber self-identified as Irish.[203] Regardless, due to the storage location, the MLAT procedures were available for the government to petition Ireland for access.[204] In fact, the Irish government expressed its willingness to facilitate the U.S. government's access to the content through the MLAT procedure.[205]

The Google cases, on the other hand, involve electronic data that is sharded and distributed in pieces to servers throughout the world.[206] This means that such data may only be recognizable after Google reconstructs it.[207] The record in some cases indicates that the only Google personnel authorized to access the data shards are located in the United States.[208] These elements of Google's network animate the policy concerns of many of the judges who are worried about sanctioning a situation in which neither the United States nor any other nation may access the data in question.[209] Not only would pursuing the MLAT procedure lead to "a global game of whack-a-mole" but "the MLAT process would be useless because, as Google states, the only

200. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53, 72 (2d Cir. 2017) (Raggi, J., dissenting).

201. *See id.*; *In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757 (GMH), 2017 WL 2480752, at *10 (D.D.C. June 2, 2017), *aff'd*, No. 16-mj-00757 (BAH), 2017 WL 3445634 (D.D.C. July 31, 2017). Google has argued that it does *not* act as an agent of the government when it retrieves records from the overseas storage location, complicating the company's reliance on *Microsoft I*. *See In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 2480752, at *10.

202. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 200 (2d Cir. 2016), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

203. *Id.* at 230 (Lynch, J., concurring) (explaining that Microsoft "relies . . . on customers' self-reporting in classifying customers by residence, and stores emails (but only for the most part . . .) on local servers").

204. *See supra* note 154 and accompanying text.

205. Brief for Ireland as Amicus Curiae at 4, *Microsoft I*, 829 F.3d 197 (No. 14-2985-CV).

206. *See In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *2; *see also supra* Part I.A.

207. *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *2 (D.N.J. July 10, 2017).

208. *See In re Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc.*, 2017 WL 3445634, at *26.

209. *See id.*

personnel with the authority to access user communications are located in the United States."[210]

II. THE POSSIBLE OUTCOMES OF *MICROSOFT* AND CALLS FOR LEGISLATIVE ACTION

On February 27, 2018, the Supreme Court will hear oral arguments in *Microsoft*.[211] Few, however, are optimistic that resolution of this case will solve the broader challenges posed by global cloud storage networks. Some of the judges who authored the opinions discussed in Part I expressed their belief that, more than anything, Congress needs to act in this area.[212] Not even major service providers like Google or Microsoft think that the *Microsoft I* verdict creates a viable standard moving forward.[213] Many law enforcement officials have voiced concerns and described the negative effects that this decision has had on their ability to conduct investigations.[214]

Part II.A below discusses the limited judicial options for resolving *Microsoft* and suggests that statutory protections might be a better fit for new technologies. Part II.B then describes what the stakeholders in this debate would want out of such legislation. Finally, Part II.C discusses a legislative proposal to amend the SCA—the International Communications Privacy Act.

A. The Supreme Court's Limited Options in Microsoft

In *Microsoft*, the Supreme Court must choose between two positions, both having far-reaching implications.[215] On the one hand, a verdict for Microsoft may arbitrarily limit legitimate law enforcement investigations, potentially forcing officials (who have satisfied the probable cause requirement) to petition foreign governments for records pertaining to U.S. citizens.[216] On the other hand, a verdict for the government would "broadcast to the world

210. *Id.*; *see also In re* Search of Content That Is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *2 (N.D. Cal. Apr. 25, 2017) ("[O]nly Google personnel on the [U.S.-based legal] team are authorized to access and produce the content of communications."), *aff'd*, No. 16-mc-80263-RS, 2017 WL 3478809 (N.D. Cal. Aug. 14, 2017).

211. *Docket No. 17-2*, *supra* note 12.

212. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53, 55 (2d Cir. 2017) (Carney, J., concurring) ("We recognize at the same time that in many ways the SCA has been left behind by technology. It is overdue for a congressional revision that would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose."); Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 233 (2d Cir. 2016) (Lynch, J., concurring) ("Although I believe that we have reached the correct result as a matter of interpreting the statute before us, I believe even more strongly that the statute should be revised . . . ."), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

213. *See* Smith, *supra* note 3.

214. *See, e.g.*, Brief for the States of Vermont et al. as Amici Curiae Supporting Petitioner at 6–17, United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

215. *See* Daskal, *supra* note 15.

216. *Id.*

that [U.S.] law enforcement can access data held by a domestically based company anywhere."[217] The potential ramifications of each of these outcomes are addressed in turn.

1. Holding for Microsoft

If the Court holds in Microsoft's favor, providers could continue to invoke the decision and deny government requests for data that are stored abroad, no matter the strength of the government's probable cause argument.[218] If the holding is broad, this would remain true even if both sender and recipient were U.S. citizens located in the United States.[219] Judges and law enforcement officials have noted that this is a troubling result that potentially jeopardizes public safety.[220]

Furthermore, tying the government's access to email solely to the location where the data is stored leads to some absurd and potentially dangerous results. For example, under the system Microsoft currently uses, which allows users to "self-report" a geographic location, someone seeking to elude U.S. law enforcement could simply self-report a country outside the United States.[221] Under Google's system, which shards data and constantly moves it throughout the world, whether the government's warrant is enforceable could hinge on an automated network decision.[222] This interpretation of the SCA does not balance privacy considerations against law enforcement needs but rather places the power to control the reach of an SCA warrant exclusively in the hands of service providers.[223]

2. Holding for the Government

If the Court holds in the government's favor, U.S. law enforcement officers will have unilateral power to access the emails of anyone who uses a service provider that can be served with a warrant in the United States. Commentators fear that a holding for the government may cause other

---

217. *Id.*

218. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 224 (2d Cir. 2016) (Lynch, J., concurring), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

219. Brief for Petitioner at 42, *Microsoft Corp.*, 138 S. Ct. 356 (No. 17-2).

220. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft II*), 855 F.3d 53, 63–64 (2d Cir. 2017) (Cabranes, J., dissenting); Brief for the States of Vermont et al. as Amici Curiae Supporting Petitioner, *supra* note 214, at 8–11, 15–17 (describing incidents where providers' noncompliance with SCA warrants has impeded criminal investigations).

221. *Microsoft II*, 855 F.3d at 64.

222. *See In re* Search of Info. Associated with [redacted]@gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-00757 (BAH), 2017 WL 3445634, at *26 (D.D.C. July 31, 2017).

223. *See Microsoft I*, 829 F.3d at 223–24 ("Microsoft does not ask the Court to create, as a matter of constitutional law, stricter safeguards on the protection of those emails . . . . Rather, the sole issue involved is whether Microsoft can thwart the government's otherwise justified demand for the emails at issue by the simple expedient of choosing—in its own discretion—to store them on a server in another country.").

countries to pass stronger prohibitions on data disclosure or to reciprocate with similar unilateral access policies that implicate the privacy and security of U.S. citizens.[224] Increased localization measures and disclosure prohibitions tend to make data less secure worldwide.[225] Moreover, encouraging foreign governments to exercise the same kind of authority throughout the world has severe negative privacy implications.[226]

Holding for the government could also have negative consequences for businesses in the United States. The sale of internet-connected American exports might decline if people believe that using such products exposes them to the U.S. government's jurisdiction and bypasses local privacy standards.[227] As more products are produced with some element of internet connectivity, it is important to recognize that international perceptions about U.S. surveillance matter when companies compete for business abroad.[228]

Finally, a group of former intelligence and law enforcement officials from the United States and Europe, appearing as amici curiae in the *Microsoft* case, have explained how a holding for the government could be potentially detrimental for both service providers and law enforcement.[229] The brief explains how a verdict in favor of the government would burden service providers who do business internationally and simultaneously frustrate law enforcement efforts.[230] It argues that a company that is subject to sanctions in one country for conduct compelled by the laws of another country will typically exhaust its legal options to challenge an adverse ruling in one forum to avoid liability in the other.[231] Meanwhile, "law enforcement and investigations [are left] in limbo."[232]

3. A Possible Solution Under the All Writs Act

Professor Orin Kerr has discussed an alternative to the above potential outcomes of *Microsoft*. By analyzing the case under the All Writs Act (AWA) rather than the SCA, the Court could forge a more nuanced solution.[233] In short, he explains that it is the AWA, not the SCA, that

224. Brief of Former Law Enforcement, National Security, and Intelligence Officials as Amici Curiae in Support of Neither Party at 5, 9, *Microsoft Corp.*, 138 S. Ct. 356 (No. 17-2) [hereinafter Brief of Former Law Enforcement].

225. *See* Chander & Lê, *supra* note 33, at 719 (noting that data localization may undermine security by offering criminals the "tempting jackpot" of data gathered in a single location and favoring local providers that "may be more likely to have weak security infrastructure than companies that continuously improve their security to respond to the ever-growing sophistication of cyberthieves").

226. *See* Daskal, *supra* note 15.

227. *See* Smith, *supra* note 3; *see also* Schwartz, *supra* note 39 (manuscript at 27) ("In much of the world, the choice of a non-U.S. party for a local cloud can be considered as opting in to her domestic regulatory system—one in which she enjoys political representation.").

228. *See* Smith, *supra* note 3.

229. Brief of Former Law Enforcement, *supra* note 224, at 2–3.

230. *See id.* at 4–7.

231. *See id.* at 6.

232. *Id.*

233. *See* Kerr, *supra* note 87.

requires providers to assist the government in accessing records abroad.[234] The AWA authorizes courts to issue "all writs necessary or appropriate in aid of their respective jurisdictions and agreeable to the usages and principles of law."[235] The Court could use this flexible language to hold that providers must assist the government in obtaining the foreign-stored data of U.S. persons only, which is in line with the understanding that a court's warrant jurisdiction "does not ordinarily extend to the property of foreigners abroad."[236]

While this is one potential solution, the argument was not raised below and departs from the question on which the Court granted certiorari. If the case were resolved in this way, it would either have to be remanded and reheard (delaying the ultimate result, likely for years), or the Court would have to take the rare course of asking the parties for supplemental briefing.[237]

Professor Jennifer Daskal disagrees with Professor Kerr and has argued that the AWA is not a viable solution.[238] She argues that the SCA does, in fact, compel the provider to retrieve and produce the records at issue.[239] The AWA would only come into play once the Court has decided the underlying extraterritoriality issue.[240] Thus, she argues that the Court remains unable to reach this elegant, nuanced solution and that the legislature should act in its stead.[241]

B. The Advantages of a Legislative Solution

The outdated statute that the Justices must apply in this case limits the Court's options. The ultimate solution to the *Microsoft* problem must balance "effective law enforcement, national sovereignty, international comity, Internet openness and efficiency, commerce, and informational privacy."[242] In general, the legislature is better suited than courts to meet these challenges.

Privacy protection in the United States is derived both from the Fourth Amendment[243] and from legislation.[244] Legislation can be tailored to adapt to changing technology.[245] Legislation may also cover areas that lack Fourth Amendment protection, either because courts have declined to confront the

234. *Id.*
235. 28 U.S.C. § 1651(a) (2012).
236. *See* Kerr, *supra* note 87.
237. *Id.*
238. *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/W88B-Q2UG].
239. *Id.* ("[E]ven if the All Writs Act could have once been relied [on] to authorize the kind of search at issue in . . . *Microsoft* . . . , the SCA now governs.").
240. *Id.* ("[T]he All Writs Act doesn't and can't avoid the key issue in the case—is this a territorial or extraterritorial exercise of the government's warrant authority?").
241. *Id.*
242. Brief of Former Law Enforcement, *supra* note 224, at 2–3.
243. *See supra* Part I.B.
244. *See supra* Part I.C.
245. *See* Kerr, *supra* note 110, at 1148–49.

issue or because the specific question has not been raised.[246] For example, Congress's very intention in passing the the ECPA was to protect electronic data where the Fourth Amendment did not.[247]

Legislative bodies are also "well situated to gauge changing public attitudes, to draw detailed lines, and to balance privacy and public safety in a comprehensive way."[248] This advantage is particularly necessary when adapting to new technology, where crafting an effective policy often requires more detailed study and a deeper appreciation for the possible ramifications that different rules might have.[249]

Of course, judicial doctrines tend to move slowly and sweep broadly, and search and seizure doctrine is no exception—it takes time to develop and is difficult to reverse or limit once in place.[250] These limitations have prompted the Supreme Court to note that "[t]he judiciary risks error by elaborating too fully on the Fourth Amendment implications of emerging technology before its role in society has become clear."[251]

Concurring in the judgment in *Microsoft I*, Judge Gerard E. Lynch recognized the limits of a judicial solution and was vocal in advocating for a legislative solution.[252] His concurring opinion articulated many of the policy issues presented by this case, and he stressed that the court was limited to applying "a default rule of statutory interpretation to a statute that does not provide an explicit answer to the question before us."[253] He observed that Congress is better positioned to develop a nuanced solution,[254] and he recognized that a decision by the court for either party could lead to absurd results. He also noted that lawmakers were not so bound—unlike the court, they "need not make an all-or-nothing choice."[255]

C. Envisioning the SCA's Replacement

This Part surveys some positions taken by two of the major stakeholders who have testified before Congress on this issue—service providers and law

246. For example, despite the trend in favor of adopting the Sixth Circuit's *Warshak* holding, whether emails held by a third party can receive the full protection of the Fourth Amendment remains an open question because the Supreme Court has not squarely addressed the issue. *See supra* Part I.B.1.

247. *See supra* note 116 and accompanying text.

248. United States v. Jones, 565 U.S. 400, 429–30 (2012) (Alito, J., concurring).

249. *See* ACLU v. Clapper, 785 F.3d 787, 824 (2d Cir. 2015) (noting that "the legislative process has considerable advantages in developing knowledge about the far-reaching technological advances that render today's surveillance methods drastically different from what has existed in the past").

250. *See* Riley v. California, 134 S. Ct. 2473, 2497 (2014) (remarking that modern privacy protection should not be "left primarily to the federal courts using the blunt instrument of the Fourth Amendment").

251. City of Ontario v. Quon, 560 U.S. 746, 759 (2010).

252. Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.) (*Microsoft I*), 829 F.3d 197, 231–32 (2d Cir. 2016) (Lynch, J., concurring), *cert. granted sub nom.* United States v. Microsoft Corp., 138 S. Ct. 356 (Oct. 16, 2017) (No. 17-2).

253. *Id.* at 232.

254. *Id.*

255. *Id.*

enforcement officials. This Part also discusses some scholarly perspectives on the matter.

1. Service Providers Call for a Nuanced Legislative Solution

Some major service providers, driven by their concerns over conflicting data privacy laws and the illogical results that come from applying U.S. laws based on server location, advocate for a legislative solution.

Even in the wake of its victory in the Second Circuit, Microsoft has advocated amending the SCA.[256] Microsoft's President and Chief Legal Officer Brad Smith has noted that if the SCA is not modernized, service providers will be put in a precarious position when the EU's pending GDPR and other, similar laws make cross-border data transfers unlawful.[257] He has also raised concerns about the international reaction if the United States asserts a unilateral right to access the emails of foreign citizens.[258] Among other concerns, he fears that the resulting erosion of international trust would have a negative economic effect.[259]

Similarly, Google representative Richard Salgado testified before Congress that new legislation should focus on the location and nationality of the user and "eschew data location as a relevant consideration in determining whether a particular country can exercise jurisdiction over a service provider."[260] Based on user identity and location, he suggested a framework that would provide notice of records requests to foreign governments and give the United States reciprocal treatment.[261] If there were any concerns related to the release of certain records, this notice would provide friendly foreign governments an opportunity to raise their concerns diplomatically and perhaps even levy a challenge in a U.S. court.[262] A system where law enforcement's access to data is based on the identity of the user rather than the storage location echoes a solution proposed by several other commentators.[263] Legislative proposals like the ICPA, discussed in Part II.D, have also adopted this approach.[264]

2. Law Enforcement Officers Call for Clarity

Both federal and state governments have criticized the *Microsoft I* decision for frustrating law enforcement efforts to obtain evidence, especially in investigations "*where the victim, the offender, and the account holder are all*

256. *See* Smith, *supra* note 3 ("[Microsoft would] prefer to keep working alongside the DOJ and before Congress on enacting new law . . . that works for everyone rather than arguing about an outdated law. We think the legislative path is better for the country too.").
257. *See id.*
258. *See id.*
259. *See id.*
260. Statement, Richard Salgado, *supra* note 129, at 4.
261. *See id.* at 5.
262. *See id.*
263. *See, e.g.*, Kerr *supra* note 4, at 416; Daskal, *supra* note 15.
264. *See infra* Part II.D.

within the United States."[265] The DOJ has proclaimed that the Second Circuit's holding has thwarted legitimate law enforcement efforts in cases where companies have withheld data.[266] Examples include cases where quick access to the records would have helped to identify and locate child exploitation victims, locate a fugitive who skipped bail before standing trial in a child pornography prosecution, and discover coconspirators in a case involving hacking and stolen identities.[267]

The DOJ has suggested amending the SCA so that the law would apply in the manner that it did prior to *Microsoft I*.[268] Speaking before the Senate on behalf of the DOJ, Deputy Assistant Attorney General Brad Wiegmann downplayed concerns about international comity and conflicts of law, stating that those problems "are traditionally avoided through mechanisms such as prosecutorial discretion, court supervision, diplomacy, and economic considerations."[269] In his estimation, new legislation that is too concerned with comity would likely tie law enforcement's hands and would be inconsistent with the way other countries treat their domestic providers.[270]

Professor Andrew Keane Woods has advocated a similar approach. He has suggested clarification that SCA warrants only "operate" at the place where law enforcement searches or seizes the data (i.e., the domestic location where law enforcement officers actually are given the data by the provider).[271] He further suggests that an alternative approach would be to explicitly declare that SCA warrants do have extraterritorial reach in *Microsoft*-like circumstances.[272] Similar to Deputy Assistant Director Wiegmann, Professor Woods believes that the concerns over conflicts of law are overstated and easily dealt with by traditional judicial mechanisms.[273] He analogizes the records at issue here to banking records.[274] This analysis is

265. Statement, Brad Wiegmann, Deputy Assistant Attorney Gen. of the U.S., Hearing Before the Senate Subcommittee on Crime and Terrorism of the Senate Committee on the Judiciary, Law Enforcement Access to Data Stored Across Borders: Facilitating Cooperation and Protecting Rights 6 (May 24, 2017) (unpublished testimony), https://www.judiciary.senate.gov/imo/media/doc/05-24-7%20Wiegmann%20Testimony.pdf [https://perma.cc/6W7Y-DW7V]; *see also* Brief for the States of Vermont et al. as Amici Curiae Supporting Petitioner, *supra* note 214, at 6–17.

266. *See* Statement, Brad Wiegmann, *supra* note 265, at 5–6.

267. *Id.*

268. *See id.* at 10.

269. *Id.* He also argues that international practice is to allow law enforcement to compel domestic providers to produce data stored outside the country. *Id.* at 11–12.

270. *Id.* at 10.

271. *See* Statement, Andrew Keane Woods, Assistant Professor, Univ. of Ky. Coll. of Law, Hearing Before the House Committee on the Judiciary, Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era 5 (June 15, 2017) (unpublished testimony), https://judiciary.house.gov/wp-content/uploads/2017/06/Woods-Testimony.pdf [https://perma.cc/JW7U-BKXX] ("[T]he warrant would compel production in whatever American jurisdiction Microsoft received the warrant—but it would be agnostic as to the location that Microsoft has chosen to store the data.").

272. *See id.*

273. *See id.* at 6 ("When there is a conflict with another country's laws, courts have equitable tools at their disposal—doctrines like comity—that allow them to weigh the competing equities in a given case.").

274. *See id.* at 5–6.

consistent with his position that "[m]any of the features that are cited as evidence of data's unique properties are in fact neither novel nor unique to data."[275]

D. Proposed Legislation: The International Communications Privacy Act

A legislative effort to amend the SCA in response to the concerns raised above is underway.[276] The version of the ICPA discussed in this Part[277] was introduced in the Senate on July 27, 2017,[278] and in the House on September 8, 2017.[279] The bipartisan bill explicitly acknowledges that legislation in this area needs to consider the legitimate needs of U.S. law enforcement agencies, the privacy interests of customers, and the interest foreign governments have in protecting their citizens' "human rights, civil liberties and privacy."[280] The ICPA would require a warrant for all contents of stored data, regardless of where they are stored.[281] It also would provide comity-based procedural protections to users who are located outside the United States and are determined to be nationals of "qualifying foreign countr[ies]."[282]

The ICPA would make the location of data storage irrelevant to the determination whether U.S. law enforcement can compel production of the data.[283] Rather, any provider that stores data[284] could be compelled to disclose the contents of that data with a warrant, provided that the

275. Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 756 (2016).

276. *See* International Communications Privacy Act, H.R. 3718, 115th Cong. (2017); International Communications Privacy Act, S. 1671, 115th Cong. (2017). As noted above, an updated version of this legislation has been introduced in the form of the CLOUD Act. *See supra* note 27. This Part primarily discusses the ICPA but notes some of the differences between the two bills.

277. Previous versions of the bill were introduced in both chambers. *See* H.R. 5323, 114th Cong. (2016); S. 2986, 114th Cong. (2016).

278. S. 1671.

279. H.R. 3718.

280. *Id.* § 2(3)(C); S. 1671 § 2(3)(C).

281. *See* H.R. 3718 § 3(a)(2)(A); S. 1671 § 3(a)(2)(A). The CLOUD Act does not explicitly provide that law enforcement must have a warrant obtain the contents of electronic communications. *See* CLOUD Act, H.R. 4943 § 3(a)(1), 115th Cong. (2018); CLOUD Act, S. 2383 § 3(a)(1), 115th Cong. (2018).

282. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). "Qualifying foreign countries" under the ICPA would guarantee to the United States that they would handle records requests in compliance with certain guidelines and would have their "qualifying" status approved by the Attorney General with the advice of the Secretary of State. *See infra* notes 288–91 and accompanying text.

283. H.R. 3718 § 3(a)(2)(A); S. 1671 § 3(a)(2)(A) ("A governmental entity may require the disclosure . . . of the contents of a wire or electronic communication . . . regardless of where such contents may be in electronic storage or otherwise stored, held, or maintained . . . ."). The CLOUD Act likewise provides that service providers must disclose records in compliance with a warrant regardless of storage location. *See* H.R. 4943 § 3(a)(1); S. 2383 § 3(a)(1).

284. The amended provision would cover both ECS and RCS, flattening the problematic distinction discussed above in Part I.C.1.

governmental entity has jurisdiction over the offense.[285] Such a warrant would be "issued using the procedures described in the Federal Rules of Criminal Procedure."[286]

Under the ICPA, the Attorney General would publish a list of "qualifying foreign countries" who have a qualified right[287] to be notified of, and file an objection to, warrants issued for records of their non-U.S.-located nationals.[288] To qualify, a foreign government would agree not to notify the target subscriber of the warrant or the investigation.[289] The foreign government would also have to agree to handle requests for any U.S. person's data in a reciprocal fashion.[290] Finally, the Attorney General would also consult with the Secretary of State to determine whether the country has sufficient privacy, civil liberties, and human rights protections; whether the country has a record of cooperating with the U.S. government; and whether it can be counted on not to impede U.S. investigations or undermine U.S. foreign relations if it did receive notice of a warrant.[291]

Assuming at least one country "qualifies" under the ICPA's criteria, the bill would require that warrants state the "nationality and location" of the subscriber whose records are to be released.[292] If that information could not "reasonably be determined," the warrant would have to include "a full and complete statement of the investigative steps" that proved unsuccessful in determining the subscriber's location and nationality.[293] However, this requirement would only benefit qualifying countries.[294] If no foreign country

285. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D). "Jurisdiction over [the] offense" for domestic law enforcement is defined as "an investigation of a criminal offense for which [a particular governmental entity] has jurisdiction." H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

286. H.R. 3718 § 3(a)(2)(A); S. 1671 § 3(a)(2)(A).

287. The default rule under the ICPA would be that qualifying foreign countries must receive notification. *See* H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). However, the bill provides for access to records with delayed notification to the qualifying foreign country where notice would jeopardize national security or where it is believed that the foreign government is involved in the investigated activity or would notify the subscriber of the existence of the investigation or warrant. *See* H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). The CLOUD Act would permit a service provider to notify a qualifying foreign government of a request for one of its nationals' or residents' records, but unlike the ICPA it does not *require* such notification. H.R. 4943 § 3(b); S. 2383 § 3(b).

288. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

289. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

290. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). In the ICPA, the term "U.S. person" encompasses "citizen[s] of the United States or . . . alien[s] lawfully admitted for permanent residence." H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

291. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

292. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

293. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D). Departing from the ICPA, the CLOUD Act does not place the burden of attempting to determine a target's nationality on law enforcement officers. *See* CLOUD Act, H.R. 4943 § 3(b), 115th Cong. (2018); CLOUD Act, S. 2383 § 3(b), 115th Cong. (2018). Rather, the updated proposal makes it incumbent upon the service provider to move to quash a warrant that would require it to violate a qualifying foreign country's laws. *See* H.R. 4943 § 3(b); S. 2383 § 3(b). Qualifying foreign governments under the CLOUD Act would have to guarantee reciprocal treatment of U.S. law enforcement requests and enter into a formal executive agreement with the United States, the terms of which are set out in detail in the bill. *See* H.R. 4943 §§ 3(b), 5(a); S. 2383 §§ 3(b), 5(a).

294. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

qualifies, then the default rule would require disclosure of the requested data upon service of a warrant on the provider.[295] In such a situation, the warrant would not need to mention the subscriber's nationality, location, or what steps were taken in an attempt to determine that information.[296]

Both service providers and qualifying foreign countries would be able to object to the release of records under the ICPA.[297] If a warrant under the ICPA sought the records of a non-U.S.-located national of a qualifying foreign country, the U.S. government would be required to notify the foreign country's "Central Authority."[298] The notice would have to include the name, nationality, and location of the subscriber and service provider, as well as an explanation of the relevant events and why records are sought.[299] However, a qualifying foreign country could not unilaterally quash the warrant. A country or service provider objecting to the warrant would first have to demonstrate that compliance would violate "the laws of a foreign country."[300] If disclosure would be illegal under the relevant country's laws, the court would have to weigh the foreign country's and provider's interests against those of the U.S. government.[301]

Thus, the ICPA would both expand and contract the government's existing warrant power under the SCA. The bill divorces the reach of the warrant from the data's storage location, which gives the government the ability to investigate any crime over which it has jurisdiction.[302] Before getting the warrant, however, the government would have to make a good-faith effort to determine the nationality of its target and, if the subscriber is a national of a certain foreign country, that country's government or the service provider could move to quash or modify the warrant.[303]

---

295. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

296. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

297. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

298. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). "Central Authority" is defined as "the agency, department, office, or authority of a country responsible for administering law enforcement requests between that country and another country." H.R. 3718 § 3(a)(5)(C); S. 1671 § 3(a)(5)(C).

299. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

300. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

301. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). The comity factors listed in the bill are laws of the foreign country; investigative interests of the U.S. governmental entity seeking to compel disclosure; the foreign government's interest in preventing the disclosure; the foreign government's reasons for objecting, if any; penalties the provider or its employees would suffer for violating foreign laws; location and nationality of subscriber or customer whose communications are sought; location and nationality of the victims; location of the offense; seriousness of the offense; importance of the sought-after data to the investigation; and the possibility of timely accessing the data through alternative means. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3). The CLOUD Act provides for a similar comity analysis where a provider can show that there is a "material risk" that disclosing records would violate the laws of a qualifying foreign country. *See* CLOUD Act, H.R. 4943 § 3(b), 115th Cong. (2018); CLOUD Act, S. 2383 § 3(b), 115th Cong. (2018). The CLOUD Act also clarifies that any comity analysis that would be available under common law would remain available under the Act. H.R. 4943 § 3(c); S. 2383 § 3(c)**.**

302. H.R. 3718 § 3(a)(2)(D); S. 1671 § 3(a)(2)(D).

303. H.R. 3718 § 3(a)(3); S. 1671 § 3(a)(3).

III. A LEGISLATIVE SOLUTION THAT SEPARATES DOMESTIC AND FOREIGN SEARCHES ON THE BASIS OF USER IDENTITY

This term, the Supreme Court is set to address the question "[w]hether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. § 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad."[304] The answer will settle a question of statutory interpretation, but it is unlikely to solve the deeper issue of how the law should treat data that can be stored worldwide with no geographic connection to its owner.[305] Interpretations of existing law either grant protections based on unpredictable and (from the perspective of many subscribers) arbitrary location of a server or permit law enforcement to unilaterally collect the data of foreign citizens stored abroad.[306]

In the long term, the SCA simply cannot be stretched far enough to address the relevant equities—hence calls from all quarters for its amendment.[307] Given the limitations of the current statute[308] and the legal doctrines that courts have at their disposal,[309] no judicial response can fully address the issues at play. The SCA's vague language leaves too much space for the interposition of traditional warrant and subpoena doctrines,[310] neither of which is a perfect fit given the nature of this technology. Traditional warrant doctrines are tied to the physical world, and the territoriality question raised in *Microsoft* eludes any easy answer grounded in the operation of traditional search warrants.[311] Likewise, the subpoena analogy does not quite fit in the context of a statute that was intended to give the contents of communications greater protection than a subpoena typically provides.[312]

Similarly, the presumption against extraterritoriality has mostly muddled this issue.[313] Though the Supreme Court must interpret the SCA in light of its precedent and canons, this will not solve the underlying problems of a statute that is past its expiration date.[314] Ultimately, the legislature is best equipped to draw lines and establish rules that are needed to govern access to this complex and still-developing technology.[315] Therefore, this Part proposes a legislative solution that modifies the proposed ICPA.

304. Petition for Writ of Certiorari at I, United States v. Microsoft Corp., 138 S. Ct. 356 (2017) (No. 17-2).
305. *See supra* Part I.A.1.
306. *See supra* Part II.A.1.
307. *See supra* Part II.C.
308. *See supra* Part I.C.
309. *See supra* Parts I.B, I.D.
310. *See supra* Part I.B.
311. *See supra* Part I.D.
312. *See supra* Part I.C.
313. *See supra* Part I.D.
314. *See supra* Part II.
315. *See supra* Part II.B.

A. What the ICPA Gets Right and What It Lacks

The ICPA provides a good framework and starting place for discussion, as it already incorporates two important features: (1) a probable cause warrant requirement for all communicative content and (2) a user-nationality-based system for determining the reach of warrants.[316] However, the statute may fail to obviate fears from the rest of the world that law enforcement in the United States is using service providers located here to reach the records of foreign citizens located abroad.[317]

The ICPA addresses the specific problem raised in *Microsoft*: the text of the bill states that warrants for electronic data would be effective regardless of the storage location of the records.[318] The bill also provides some comity-based safeguards in the form of its notice requirement and a balancing test in response to objections from some countries.[319]

One problem with the ICPA is that, beneath the notice requirement and the comity balancing test, there is still a default presumption that U.S. law enforcement should have access to the records of foreign nationals that are not stored in the United States.[320] Thus, the act conflates, in certain circumstances, two sets of subscribers who are in very different positions: U.S. citizens and residents who are rationally governed by U.S. laws and law enforcement on the one hand and foreign citizens whose only connection to the United States is a service provider doing business there on the other. While law enforcement should be able to access the latter group's records in some instances, international comity justifies some additional procedural safeguards.

B. Governing Access to United States and Foreign User Data with Fully Separate Procedures

This Note suggests the creation of two distinct forms of legal process, one governing primarily "domestic" requests and another governing wholly extraterritorial requests. Creating a separate order for obtaining the records of a foreign person stored outside the United States would clarify the bill and allow the law to deal with these distinct groups on different terms.[321]

---

316. *See supra* notes 281–82 and accompanying text; *see also supra* notes 292–93 and accompanying text. The updated legislative proposal, the CLOUD Act, would not explicitly require a warrant for the contents of data. *See supra* note 281. Under the CLOUD Act, a user's identity could possibly be grounds to limit the reach of a warrant but that bill's identity-based protections are less robust than the ICPA's. *See supra* note 293 and accompanying text.

317. *See supra* Parts I.A.2, II.A.2.

318. *See supra* notes 283, 285 and accompanying text. The CLOUD Act has a similar provision. *See supra* note 283.

319. *See supra* notes 288–301 and accompanying text. The CLOUD Act permits a provider to notify a qualifying foreign government of a request in certain circumstances but does not require notice. *See supra* note 287. The CLOUD Act also would allow courts to engage in a comity analysis if certain conditions are met or if such an analysis would be appropriate under common law. *See supra* notes 293, 301.

320. *See supra* notes 292–96 and accompanying text. This would also be the default presumption under the CLOUD Act. *See supra* note 293.

321. The choice to call the domestic instrument a "warrant" and the extraterritorial instrument an "order" signals that domestically, the traditional Fourth Amendment limits

Under this proposal, the law would provide for two separate investigative instruments: a "domestic warrant" that applies to the records of U.S. persons[322] regardless of where those records are stored and an "international order"—a separate court order to investigate foreign conduct having substantial U.S. effects. The government would apply for the international order when it was unable to demonstrate that the records belong to a U.S. person. Therefore, much like the ICPA, part of the application process for either of these instruments would involve the government establishing the nationality and location of the user.

1. The Domestic Warrant

Qualifying for the domestic warrant would require probable cause, including a showing that the subscriber whose information is sought is a U.S. person. Upon that showing a warrant would issue, and the provider would be required to disclose the content regardless of its storage location. The reach of this domestic warrant would be clear, and it would have the additional privacy benefit of invoking traditional Fourth Amendment protections.[323]

2. The International Order

For foreign citizens, two safeguards would ensure that records are not disclosed in violation of another nation's sovereignty or privacy laws. First, the international order would require probable cause to obtain the records and require detailed evidence as to the domestic effects of the investigated crime. This requirement intends to make judges gatekeepers charged with conducting a comity-like analysis prior to issuing the international order, during which they would weigh U.S. law enforcement interests against foreign sovereignty interests.[324]

Second, once an international order was issued, a provider would be allowed to deny[325] the request on a showing that compliance would violate the privacy laws of the nation at issue. The burden would rest on the provider

---

govern the warrant. Calling the extraterritorial instrument an "order" does not imply less probable cause protection but recognizes the extraterritorial limits on warrants and the Fourth Amendment.

322. The term "U.S. persons" as used throughout this Part refers to citizens and permanent residents of the United States. *See supra* note 29 and accompanying text.

323. *See supra* Part I.B.1.

324. The extent of the suspect's contacts with the United States, including his or her presence within the United States during the investigation, would factor into the comity analysis. The comity analysis also addresses the situation where a user is anonymous—where there is no competing foreign interest (because the user's nationality and location are unknown), U.S. law enforcement interests will weigh more heavily in the interest of issuing the order.

325. This would not affect counterterrorism surveillance pursuant to FISA. *See supra* note 111 and accompanying text.

to produce evidence of conflicting foreign law.[326] This default rule shows regard for the laws of other nations and recognizes that the U.S. government is not acting unilaterally. Rather, it would be compelling the action of a third-party provider who is subject to the laws of multiple jurisdictions.

With these default rules in place, the statute would also leave space for diplomatic efforts to develop procedures specific to certain countries, or groups of countries, that could be negotiated in the form of bilateral or multilateral reciprocal agreements. These procedures might include a notice requirement, a relaxation of the heightened domestic effect showing, or expedited processing.

3. The Warrant and International Order System: Benefits of Separate Procedures

The major benefit of this system would be clarity for all parties involved and a built-in comity analysis that would not require a challenge to the underlying warrant. This system would also address the presumption against extraterritoriality by explicitly setting forth when and how each order would apply in contexts that are arguably extraterritorial. There would be no ambiguity that would trigger the *Morrison* test.[327] This would resolve the central debate of *Microsoft* in a nuanced way that would be difficult for the Court to get to on its own.[328] Additionally, this system would give clear notice to providers in structuring their compliance procedures and would prevent providers from storing records abroad in a manner that would preclude their release.

Law enforcement officers, likewise, would have clear notice of the limits of each of the two forms of legal process. For cases where there is no foreign element, the process would be more streamlined and prevent the possibility of objections based on storage location. Any additional burden to U.S. law enforcement would only arise in cases where it ought to—where the reach of U.S. law enforcement is legitimately questionable. Even given this necessary limitation, the statute would only preclude law enforcement officers from accessing records without foreign assistance in limited circumstances. Moreover, the executive branch would remain free to alleviate much of the burden by entering into more effective international agreements where necessary.

Users of these services in the United States would know that a modern statutory framework is in place to protect their privacy against unreasonable government intrusion, separate from the development of Fourth Amendment doctrine.[329] A consistent level of privacy protection would apply to every U.S. customer's records. Similarly, although the probable cause protection

326. For this safeguard to take effect, there would have to be a "true conflict," making it impossible for the provider to comply with both countries' laws simultaneously. *Cf.* Hartford Fire Ins. Co. v. California, 509 U.S. 764, 798–99 (1993).

327. *See supra* notes 147–52 and accompanying text.

328. *See supra* Parts II.A–B.

329. *See supra* Part I.B.1.

for the international order would not necessarily have constitutional backing,[330] it would demonstrate a good-faith commitment to personal privacy and assuage fears abroad of limitless U.S. surveillance.

Finally, this enhanced baseline for access to foreign records would give both foreign governments and their citizens assurance that they are not being spied on by U.S. law enforcement agencies simply by choosing to use a U.S.-based service provider. By taking comity into account before any order is issued, and by establishing a procedure to object when a data transfer would violate local law, the statute would have both the appearance and effect of according due respect to foreign privacy and data security laws.

CONCLUSION

Cloud technology is increasingly pervasive in modern life around the world,[331] but the law that governs a significant aspect of this technology in the United States has failed to keep pace.[332] The statute that regulates law enforcement's access to communications stored by cloud technology is out of date and eludes any interpretation that would allow for a meaningful extraterritoriality analysis.[333] The *Microsoft* opinions in the Second Circuit demonstrate the way that the statute forces courts to take an all-or-nothing position based on the often arbitrary decision service providers make about where to physically store data.[334]

Due to legislative shortcomings and a general institutional disadvantage, courts are ill equipped on their own to draw the necessary lines between those who should be primarily governed by U.S. laws and those whose governments have a right to expect that their own laws will govern. These are issues that deserve a thoughtful legislative study that accounts for all of the various privacy, sovereignty, and law enforcement equities at play.

A lasting and effective solution to the question of what limits the law places on U.S. law enforcement's reach into the cloud should come in the form of legislation that replaces the outdated SCA.[335] The ICPA provides a good starting point, but that bill still conflates foreign subscribers of service providers located in the United States with U.S. persons.[336] The law should deal with each of these two groups, which have different expectations about privacy and are subject to different levels of constitutional protection, on their own terms.[337]

Creating two separate investigative tools—one that is unconcerned with international comity by default because it governs only the records of U.S. persons and another that has built-in checks on extraterritorial extension of U.S. searches and seizures—clarifies the law for providers, law enforcement,

330. *See supra* Part I.B.1.
331. *See supra* note 38 and accompanying text.
332. *See supra* Part I.D.
333. *See supra* Part I.D.
334. *See supra* Parts I.D, II.A.1–2.
335. *See supra* Parts II.B–D.
336. *See supra* Part III.A.
337. *See supra* Part III.B.

and foreign governments.[338] It helps to ensure that U.S. service providers will be able to continue doing business abroad without having to choose between foreign data privacy laws and U.S. investigative demands.[339] Further, it demonstrates respect for foreign sovereignty and encourages international cooperation while discouraging defensive data localization measures.[340] This two-prong framework addresses the shortcomings in the current legislation and provides a logical system for governing law enforcement access to cloud data.

338. *See supra* Part III.B.3.
339. *See supra* Part III.B.3.
340. *See supra* Part III.B.3.