DRAWING LINES IN THE CLOUD: 
IMPLICATIONS OF EXTRATERRITORIAL LIMITS TO THE STORED 
COMMUNICATIONS ACT 

ANDREW J. PECORARO†

ABSTRACT 

Just how private are individuals’ private email accounts? This question has become more relevant in light of the Edward Snowden leaks in 2013, revealing that the United States was bulk-collecting the information of not only foreigners, but also the information of its own citizens. Courts have struggled to strike the right balance between practical concerns of privacy, on one hand, and the government’s legitimate interest in prosecuting crimes on the other. These complex considerations are only multiplied when a case involves access to data stored across borders. Recently, the Second Circuit departed from other case holdings to find that the presumption of extraterritoriality prevents the government from using Stored Communication Act ("SCA") warrants—or perhaps any domestic legal process—to access data that is stored overseas.

This Article explores the rationale employed by the Second Circuit and other cases to conclude that such decisions will have significant implications for other provisions of the SCA and potentially undermine long-standing Fourth Amendment doctrines, such as the Bank of Nova Scotia doctrine and the third-party doctrine. This Article highlights two conclusions that may impact these other doctrines: first, the conclusion that a provider accessing data on one of its servers constitutes a search under the Fourth Amendment; and second, that the location of the data is a determinative factor in deciding jurisdiction over that data.

Arguing against the prevailing trend in the academic literature in this area, this Article concludes that providers’ access to their own servers cannot be a search under the Fourth Amendment and, further, that

† J.D., May 2017, William & Mary Law School; M. Litt., May 2010, University of Glasgow; B.A., May 2005, McDaniel College. Thanks to Judge David J. Novak, Paul Marcus, Adam Gershowitz, Janet Smith, and Mary Catherine Amerine for helpful comments, and suggestions. This Article benefited from presentation to the National Security Law class at William & Mary Law School. The opinions contained herein are my own, at the time of writing, and do not necessarily reflect the opinion of any individual listed above, any employer, or any other organization with whom I am affiliated. All errors are my own.
the location of data is a problematic factor to rely upon. It argues that the SCA should be interpreted to reach data stored overseas held by electronic service providers that are subject to U.S. jurisdiction. It argues that the jurisdictional test for what service providers should be subject to the SCA obligation is much narrower than currently employed and should follow from cases such as Daimler A.G. v. Baumer and its progeny. Further, it proposes a new test for the validity of SCA warrants, positing that such warrants should be quashed upon a prima facie showing that either the target of the investigation is not a U.S. national or the target is not acting in the United States, or that retrieving the data would violate the laws of the country in which the data is being stored. Such a proposal allows law enforcement the flexibility to investigate as needed, but respects both the international sovereignty of other nations and the privacy interests of the owners of the data.

I. INTRODUCTION ................................... 77

II. GOVERNMENT ACCESS TO ELECTRONIC
DATA .............................................. 82
   A. THE STORED COMMUNICATIONS ACT ............. 83
   B. THE PRESUMPTION AGAINST
      EXTRATERRITORIALITY AND THE SCA ........... 85
         1. Is the SCA Intended to Operate
            Extraterritorially? .......................... 87
         2. What is the Focus of the SCA? ............... 90
         3. Does an SCA Disclosure Occur
            Extraterritorially? .......................... 92

III. THE IMPLICATIONS FOR THE SCA AND THE
FOURTH AMENDMENT .............................. 96
   A. THE SCA SUBPOENA AND COURT ORDER
      PROVISIONS .................................... 96
   B. THE BANK OF NOVA SCOTIA DOCTRINE .......... 99
   C. THE THIRD-PARTY DOCTRINE .................... 102

IV. MOVING FORWARD WITH THE SCA ............. 104
   A. PROBLEMS WITH DATA AS DETERMINANT .......... 105
   B. A NEW APPROACH FOR ASSESSING JURISDICTION
      OF SCA WARRANTS ............................. 109
         1. Focusing on the Nationality of the Target .... 109
         2. Focusing on the Location of the Service
            Provider ..................................... 111

V. CONCLUSION ..................................... 117
I. INTRODUCTION

People are more attached to their electronic devices, and expect those devices—and the information they contain—to be available at a moment’s notice, connecting “seamlessly and continuously through the ‘Internet of Everything.’” Customers have the option of storing emails on private servers in their home or business, or electing to have their service provider host and store all their private communications. Companies have gone from being single-solution specialists to offering full-service storage and security for the private email accounts of their customers.

But just how private are these commercial email accounts? This question has become more relevant due to Edward Snowden’s leaks in 2013, which revealed that the United States was bulk-collecting the information of not only foreigners, but also the information of its own citizens. People began to question when, how, why, and even if the government should be able to access electronic data about an individual. And just as relevant, when should law enforcement be able to go to your service provider—Microsoft, Google, Apple, etc.—and demand that the provider disclose the contents of an email account?

In light of allegations that technology firms cooperated with this massive surveillance, these companies have begun to push back against giving the government access to their customers’ data. In addition to the straightforward privacy issues, these companies have a

---

1. See Radicati Grp., Inc., Email Statistics Report, 2012-2016 2 (2012), http://www.radicati.com/wp/wp-content/uploads/2012/04/Email-Statistics-Report-2012-2016-Executive-Summary.pdf (finding that there were approximately 3.3 billion email accounts in the world, with that number expected to increase by six percent each year).
5. Id. This type of intelligence gathering was a whiplash response to the fervor that followed the terrorist attacks of September 11, 2001. The government granted wide-spread powers to its intelligence agencies to conduct a War on Terror. See Jason Young Green, Note, Railing Against Cyber Imperialism: Discussing the Issues Surrounding the Pending Appeal of United States v. Microsoft Corp., 16 N.C. J.L. & Tech. 172, 173 (2015).
practical interest in protecting the data that they are entrusted; they fear losing massive amounts of foreign business if they are seen to be “in the pocket” of the U.S. government. Therefore, companies like Nokia, Google, and Apple have been announcing their independence from the government. Nokia, in particular, has adopted policies reaffirming its commitment to its customers’ privacy and demanding more government transparency regarding surveillance methods. Similarly, several nations are considering, or have passed, mandatory data localization requirements, pursuant to which companies doing business in their jurisdiction are required to store certain data, or copies of such data, locally. These laws and policies are aimed at preventing the United States from being able to obtain an individual’s data from a third party, particularly without informing the individual.

Such action, while appealing to privacy concerns, raises significant issues for law enforcement. When investigating serious crimes, law enforcement officers are often stymied by the sophisticated communications offenders use to plan their crimes. Often the only evidence investigators begin with is a snippet of electronic information or part of a communication concerning illicit activity; as will be discussed below, the identity and even the citizenship of suspects is often unknown. Thus, law enforcement claims that access to data is imperative for the government to be able to conduct effective investigations.

In response to this need, the government enacted statutes that allow law enforcement to obtain this information. The Electronic

---


11. See Microsoft v. United States Webinar, GEO. WASH. U. (Sept. 8, 2016), https://vimeo.com/183876113?cfcee14065 [hereinafter Webinar]. This webinar included representatives from legal academia, the U.S. Department of Justice, and attorneys that represented Microsoft. While informative, the statements of the participants should not be taken as the official position of the U.S. government, Microsoft, or any of the law firms involved in this, or any other, litigation.

12. See infra Part III.B.

Communications Privacy Act14 (“ECPA”) is a part of that law enforcement arsenal.15 Title II of the ECPA is the Stored Communications Act16 (“SCA”), which “protects the privacy of the files stored by service providers” but permits law enforcement to obtain these electronic files under narrow circumstances.17 Far from the bulk data collection under the PATRIOT Act18 and the PRISM program,19 the SCA requires the government to tailor search warrant and subpoena requests to information that they can show are materially relevant to an ongoing investigation.20 Yet the SCA, and tools like it, were enacted before the widespread adoption of email and the introduction of the “cloud.” The provisions are outdated when applied to twenty-first-century technology and present unique challenges when examined under the traditional Fourth Amendment concept of a reasonable expectation of privacy.21 A handful of scholars are now exploring the complicated jurisdictional, privacy, and security questions that are posed by the intersection of modern technology and statutory provisions ill-equipped to handle such technology.22

Striking the right balance between these practical concerns of privacy on one hand, and the government’s interest in prosecuting crimes on the other, has proven to be a difficult task. Courts have differed in determining what privacy interest, if any, a person has in electronic

19. See Barton Gellman & Laura Poitras, U.S., British Intelligence Mining Data from Nine U.S. Internet Companies in Broad Secret Program, W ASH. P OST (June 7, 2013), https://www.washingtonpost.com/investigations/us-intelligence-mining-data-from-nine-us-internet-companies-in-broad-secret-program/2013/06/06/3a0c0da8-cebf-11e2-8845-d970cc04497_story.html. PRISM is the code name for a program under which the U.S. National Security Agency (“NSA”) collected internet communications from at least nine major U.S. internet companies. See id.
20. See 18 U.S.C. § 2703(d); Shah, supra note 13, at 545.
21. See infra Part III.
data, or if accessing such data even constitutes a search at all. Traditional tools such as warrants raise new questions about territoriality when applied to the electronic landscape, rather than to a physical location; for example, is a warrant issued in the Eastern District of Virginia violating the territorial limitations of a warrant if it allows law enforcement to gather data from a computer located in California?

These concerns are only complicated when a case involves access to data stored across borders. Courts have differed on whether having a service provider access data located outside the United States constitutes a search or seizure of that data, and if so, where the actual search or seizure takes place. For example, the United States Court of Appeals for the Second Circuit has held that the “presumption against extraterritoriality” prevents law enforcement from using an SCA warrant to force an electronic service provider to disclose data that is stored outside the borders of the United States. In that case, the court held that it is the location of the data that determines whether a search is conducted territorially. More recently, a district court in Pennsylvania disagreed with the Second Circuit, finding that, even if the data is located outside the United States, there is no actual disclosure—and therefore no seizure—of the information until it has been pulled back into the United States by the provider. Therefore, the presumption against extraterritoriality does not apply.

Indeed, every other court to consider the extraterritoriality of the SCA has

23. See, e.g., United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc); In re United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
25. District courts around the country have differed on this answer to this very question. Compare United States v. Hammond, No. 16-cr-00102, 2016 WL 7157762, at *4 (N.D. Cal. Dec. 8, 2016) (finding that such a Network Investigative Technique (“NIT”) warrant from Virginia violated the territorial limitations of Fed. R. Crim. P. 41 because the defendant was only subject to the warrant when electronic instructions were downloaded onto his computer in California), with United States v. Duncan, No. 15-cr-00414, 2016 WL 134175 (D. Or. Dec. 6, 2016) (concluding that the NIT warrant operates as a tracking device authorized under Fed. R. Crim. P. 41(b), and thus there is no territorial violation).
26. The SCA provides privacy protections for users of two types of electronic services—electronic communication services (“ECS”) and remote computing services (“RCS”). See 18 U.S.C. §§ 2510-11 (2012) (defining both ECS and RCS). For convenience, this Article will use the term “service provider” or just “provider” to refer to both ECS and RCS, unless a meaningful distinction needs to be drawn.
disagreed with the Second Circuit’s interpretation. The lack of clarity in this area of the law has led to calls for Congress to amend the SCA to address this issue, and the United States Supreme Court has now decided to resolve the dissension among lower courts.

This Article explores the rationale employed by the Second Circuit and concludes that it will have significant implications for other provisions of the SCA and potentially undermine long-standing Fourth Amendment doctrines. To be clear, this Article does not claim that the Second Circuit’s decision was wrong. Microsoft appropriately stood up for the privacy interests of its customers, who did not have standing to challenge the government access, and raised important sovereignty concerns related to the use of U.S. legal process in other countries; however, even Microsoft acknowledges that the current status quo is not a favorable state of affairs.

In contrast to the prevailing trend in the academic literature in this area, this Article identifies the competing concerns that arise if a provider accessing their own servers, even in another country, is considered a search under the Fourth Amendment, and draws some logical conclusions about how the rationale of the Second Circuit case could be used to challenge other provisions of the SCA or otherwise weaken separate Fourth Amendment doctrines.

This Article proceeds in three Parts. Part II introduces the relevant provisions of the SCA, and reviews how courts have applied the presumption of extraterritoriality in this context. This Article high-

30. See, e.g., In re The Search of Content That Is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1398279, at *1, *3-4 (N.D. Cal. Apr. 19, 2017); In re The Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238, slip op. at 3 (M.D. Fla. Apr. 7, 2017) (“A warrant issued pursuant to the Act function[s] more like a subpoena in that it requires the provider to disclose information under its control.”); see also In re The Search of Info. Associated with [Redacted]@Gmail.com That Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 2480752, at *6 (D.D.C. June 2, 2017) (“Every court outside the Second Circuit that has considered the issue has rejected the holding of Microsoft . . . .”).


lights two rationales that may impact other doctrines: (1) the conclusion that a provider accessing data on one of its servers constitutes a search under the Fourth Amendment; and (2) that the location of the data is a determinative factor in deciding jurisdiction over that data. Part III considers whether the conclusion that a provider’s own access to its servers is a search impacts both other provisions of the SCA and separate Fourth Amendment doctrine, such as the In re Grand Jury Proceedings Bank of Nova Scotia and third-party doctrines. In each circumstance, the logic undergirding the conclusion rests on a faulty premise that risks removing any privacy protections for data stored even within the United States. Finally, accepting that first conclusion, Part IV then considers problems that arise when the location of data is the determinant for whether the SCA can jurisdictionally apply.

This Article concludes that the location of data is a problematic factor to rely upon and argues that the SCA should be interpreted to reach data stored overseas held by electronic service providers that are subject to U.S. jurisdiction, but that such a warrant should be quashed upon a prima facie showing that the target of the investigation is not a U.S. national or the target is not acting in the United States, or that retrieving the data would violate the laws of the country in which the data is being stored. This jurisdictional test should be more limited than the “minimum contacts” test outlined by International Shoe Co. v. Washington and its progeny. More recent cases, such as Daimler AG v. Bauman, suggest that determining what companies are subject to jurisdiction is limited to only those companies that are incorporated or headquartered in the United States, regardless of the amount of commerce that may be done here. As explained below, such a proposal allows law enforcement the flexibility to investigate as needed, but respects both the international sovereignty of other nations and the privacy interests of the owners of the data.

II. GOVERNMENT ACCESS TO ELECTRONIC DATA

The Fourth Amendment of the United States Constitution protects the right of people “to be secure in their persons, houses, papers,
and effects, against unreasonable searches and seizures.”

Yet, the Framers could not have foreseen the possibility of wireless and electronic communication. Therefore, the majority of case law and our understanding of the Fourth Amendment are inherently based on physical invasions of a person’s property.

In our modern world, however, much of our private information exists in a “virtual home,” without a clear understanding of what protections are, or should be, applied to it.

Enter the SCA, which defines a range of statutory privacy rights against access to stored account information held by network service providers.

A. THE STORED COMMUNICATIONS ACT

The SCA has long regulated government access to electronic data. Passed in 1986 as part of the ECPA, the SCA criminalizes both access to, and unauthorized disclosure of, stored communications. Although protection of electronic data is the primary purpose of the SCA, the SCA creates procedures by which law enforcement agents can lawfully compel a provider to disclose such data.

The statute provides for three different forms of legal processes—administrative subpoena, court order, and SCA warrant. Each process varies in terms of what is required for each respective process to be issued and what information each is able to compel.

An administrative subpoena is the weakest vehicle the government can use. By the terms of the statute, a subpoena can obtain a range of non-content information from service providers, including the names of the customer, addresses, payment information, and the times or durations that the customer used the service.

There is also no specific requirement or showing that the government must make in order to proceed through the use of a subpoena; the subpoena can be issued directly from an agency as “authorized by a Federal or State statute or a Federal or State grand jury.” However, the government must either notify the customer of the purposes of the subpoena, thus

---

38. U.S. CONST. amend. IV.
41. See Microsoft v. United States, 829 F.3d 197 (2d Cir. 2016), cert. granted, No.17-2, 2017 WL 2869558 (U.S. Oct. 16, 2017); see also infra Part II.B.2.
42. For a detailed analysis of the SCA, see Microsoft v. U.S., 829 F.3d 197.
44. Id. § 2703(c)(2).
45. Id. § 2703(b)(1)(A).
providing an opportunity to object to the disclosure, or obtain a court order to delay notification to use a subpoena.\textsuperscript{46}

A court order is required to obtain more detailed records about a customer’s activities, such as files detailing the contacts and email addresses with whom the customer has communicated, records of the IP addresses the customer visited over time, and other information that may implicate a third party.\textsuperscript{47} A magistrate judge issues a court order based on a finding of “specific and articulable facts” that the information sought is “relevant” to an ongoing criminal investigation.\textsuperscript{48} The heightened requirements of involving an independent member of the judiciary negates the need for notice, and thus the government is not required to notify a customer if it is only seeking non-content data as described above through a court order.

The actual content of electronic communications is reachable in two different ways, based upon the amount of time from the date the email originated. First and most relevant to this Article, in order to compel an electronic service provider to disclose the content of emails stored for 180 days or less, the government must obtain a warrant that complies with the Federal Rules of Criminal Procedure, or in the case of a state warrant, the applicable state rules.\textsuperscript{49} Second, emails that have been stored for over 180 days may be obtained through an administrative subpoena or court order only if the customer or subscriber is notified of the request.\textsuperscript{50} At the time the SCA was passed, the category of emails stored for 180 days or less was understood as covering the vast majority of stored emails; limited storage capacity meant that only a small fraction of emails would be stored past 180 days.\textsuperscript{51} Several courts have concluded, however, that as a matter of constitutional law, the warrant requirement also applies to the acquis-

\textsuperscript{46} Id. § 2703(b)(2)(c). Delayed notification allows the government to withhold notification for up to ninety days and is permitted based on finding that such notification will cause an “adverse result,” defined to include the destruction or tampering with evidence, the potential risk of flight from prosecution, a threat to or endangerment of individuals, or even undue trial delay. See id. § 2705.

\textsuperscript{47} Id. § 2703(c)(1)(E), 2703(c)(2).

\textsuperscript{48} See id. § 2703(d) (detailing the requirements of a court order).

\textsuperscript{49} Id. § 2703(a).

\textsuperscript{50} Id. § 2703(b)(1)(B). This notification could be delayed, or even prevented indefinitely, if the government can show that such notice would threaten the safety of an individual, cause the target to flee prosecution, result in the destruction of relevant evidence or intimidation of a witness, or “otherwise seriously jeopardiz[e] an investigation.” See id. § 2705.

sition of all emails, including those stored for more than 180 days and emails held by remote storage providers.52

There is no clear language within the statute itself regarding its territorial limitations, or whether the SCA was intended to apply extraterritorially. Some scholars have argued that “the legislative history, coupled with the presumption against extraterritoriality, overwhelmingly supports the conclusion that the SCA does not apply extraterritorially.”53 For example, the 1986 House Judiciary Committee Report on the SCA states that the provisions “regarding access to stored wire and electronic communications are intended to apply only to access in the territorial United States.”54 Similarly, when Congress amended the SCA in 2001 to authorize magistrate judges to issue multidistrict warrants, the amendment was titled “Nationwide Service of Search Warrants for Electronic Evidence.”55 Yet, what is unclear is how to determine the relevant location for determining extraterritoriality. In other words, “how this presumption applies when an international border separates the data and the person or entity accessing the data remains unsettled.”56

B. THE PRESCRIPTION AGAINST EXTRATERRITORIALITY AND THE SCA

The laws of the United States are generally interpreted to only apply within the territorial jurisdiction of the United States, absent a clear indication otherwise from Congress.57 This presumption grew out of the perception that Congress legislates primarily with respect to domestic affairs and so courts should decline to extend U.S. law to govern extraterritorial conduct unless explicitly instructed by Congress to do so. Indeed, it is Congress, rather than courts, that has the appropriate facilities and expertise to make policy decisions in the

52. See, e.g., United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010) (“To the extent that the SCA purports to permit the government to obtain . . . emails warrantlessly, [that portion of] the SCA is unconstitutional.”); In re Applications for Search Warrants for Case Nos. 12-MJ-8119-DJW & Info. Associated with 12-MJ-8191-DJW Target Email Address, Nos. 12-MJ-8119-DJW, 12-MJ-8191-DJW, 2012 WL 4383917, at *5 (D. Kan. Sept. 21, 2012) (“The Court finds the rationale set forth in Warshak persuasive and therefore holds that an individual has a reasonable expectation of privacy in emails or faxes stored with, sent to, or received through an electronic communications service provider.”); United States v. Ali, 870 F. Supp. 2d 10, 39 n.39 (D.D.C. 2012) (citing Warshak for the proposition that “individuals have a reasonable expectation of privacy in the content of emails stored, sent, or received through a commercial internet service provider”).
53. See, e.g., Daskal, supra note 22, at 363.
55. 18 U.S.C. §§ 2703, 2711.
56. Daskal, supra note 22, at 363.
“delicate field of international relations.” U.S. laws should be interpreted in such a way to avoid unintended conflicts with the laws of other sovereigns or to create international discord. Therefore, courts have consistently recognized that the presumption against extraterritorial application of U.S. statutes is “strong and binding.”

The United States Supreme Court, in Morrison v. National Australia Bank Ltd., set out the following two-part test for determining whether a statute has extraterritorial effect. First, does the language of the statute express a clear congressional purpose to extend the statute into areas over which the United States has no sovereign or legislative control? A clear statement signifies that Congress wants courts to apply the statute at issue to activity abroad when the court has personal jurisdiction or in rem jurisdiction over the defendant. This part of the test merely looks to see if the presumption against extraterritoriality has been rebutted. Without a “clear indication of an extraterritorial application,” the law will be presumed to have none; that is, it will not apply outside the territorial boundaries of the United States.

Second, if the language of the relevant provisions does not contemplate extraterritoriality, the court must identify the statute’s focus and determine whether the conduct at issue constitutes an unlawful extraterritorial application of that statute. If the conduct relevant to the statute’s focus occurred in the United States, then the case involves a permissible domestic application even if other conduct occurred abroad, but if the conduct relevant to the focus occurred in a foreign country, then the case involves an impermissible extraterritorial application regardless of any other conduct that occurred in U.S. territory.

While this test may facially appear to be relatively straightforward, the application of it is anything but. Scholars writing on this topic seem to agree on only one point: that the Supreme Court has

63. See RJR Nabisco, 136 S. Ct. at 2101 (reiterating that the first part of the Morrison test asks “whether the presumption against extraterritoriality has been rebutted—that is, whether the statute gives a clear, affirmative indication that it applies extraterritorially”).
64. Morrison, 561 U.S. at 255.
65. See id.
66. RJR Nabisco, 136 S. Ct. at 2101.
made a mess of this presumption. The following Parts review how courts have tried to apply this test to the SCA and particularly, to its warrant provisions.

1. Is the SCA Intended to Operate Extraterritorially?

In Microsoft v. United States, United States government authorities, in connection with an ongoing narcotics investigation within the United States, requested an SCA search warrant for the contents of a Microsoft customer's private email account. Based on the information and affidavits provided, Magistrate Judge Francis granted the warrant. The SCA warrant required Microsoft to disclose: (1) the contents of all e-mails stored in the specified user's account; (2) all records or other information regarding the identification of the user of the account; (3) all records or information stored on the account, including address books, contact lists, pictures, and files; and (4) all records of communication between the user and Microsoft.

Microsoft appropriately disclosed the information that was in the United States, but filed a motion to quash the warrant with respect to the data located overseas. Microsoft stated that because that data was located in a foreign country, such data was not within the reach of the U.S. government's authority without going through the proper international criminal procedural channels in place for retrieving documents located abroad. In effect, Microsoft challenged the

---

67. See, e.g., Anthony J. Colangelo, A Unified Approach to Extraterritoriality, 97 Va. L. Rev. 1019, 1028 (2011) (“The only thing . . . scholars [writing on the presumption against extraterritoriality] seem to agree on is that the law in this area is a mess.”); Franklin A. Gevurtz, Determining Extraterritoriality, 56 Wm. & Mary L. Rev. 341, 349-51 (2014) (“Although . . . scholars disagree regarding what the Court should do with the presumption, on one point there seems widespread agreement: the Court has made a hash of the subject.”).

68. 829 F.3d 197 (2d Cir. 2016).

69. In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 467-68 (S.D.N.Y. 2014) [hereinafter Magistrate Judge’s Decision].

70. Magistrate Judge’s Decision, 15 F. Supp. 3d at 467-68.

71. See id. at 468.

72. Id.

73. Id. at 477. The “procedural channel” referred to by Microsoft is the bilateral Mutual Legal Assistance Treaty between the United States and Ireland, facilitating the sharing of information between the two countries. See Treaty Between the Government of the United States of America and the Government of Ireland on Mutual Legal Assistance in Criminal Matters, U.S.-Ire., Jan. 18, 2001, T.I.A.S. No. 13137 [hereinafter U.S.-Ire. MLAT]. The current MLAT procedure, however, as argued by the United States and stated by Magistrate Judge Francis, is “slow and laborious, as it requires the cooperation of two governments and one of those governments may not prioritize the case as highly as the other.” Magistrate Judge’s Decision, 15 F. Supp. 3d at 474 (citing Orin S. Kerr, The Next Generation Communications Privacy Act, 162 U. Pa. L. Rev. 373, 409 (2014)).
extraterritorial application of the SCA, and specifically its warrant provision.

The magistrate judge in the *Microsoft* case initially concluded that, at least in the circumstances of that case, the SCA statute could be read to allow for extraterritorial application. The magistrate judge interpreted the “nationality principle,” which recognizes that American criminal laws can apply extraterritorially to legal entities subject to the jurisdiction of the United States, to require U.S. companies to obtain evidence located abroad that is relevant to an ongoing domestic criminal investigation. Therefore, even though the data was currently outside the United States, it was only there through the actions of Microsoft, which was subject to in personam jurisdiction of the U.S. courts, and could be compelled to pull the information back.

The magistrate judge also examined the legislative history of amendments to the SCA, finding that § 108 of the PATRIOT Act allows “nationwide service of search warrants for electronic evidence.” This expanded the SCA to allow a judge in one district, with jurisdiction over the investigation, to issue a search warrant that reached into another district, without requiring the intervention of a counterpart judge, thus expanding the reach of the magistrate judge’s power. The PATRIOT Act therefore allows a warrant under § 2703 to reach throughout the United States, so long as the provider was located within the United States. Therefore, according to the magistrate judge, it did not matter where the actual server that stored the electronic information was located. The court interpreted the focus on the location of the service provider as opposed to the location of the actual server as evidence that Congress had “anticipated that an ISP [Internet Service Provider] located in the United States would be obligated to respond to a warrant issued pursuant to § 2703(a) by producing information within its control, regardless of where that information was stored.”

The United States Court of Appeals for the Second Circuit disagreed. That court pointed out that the plain language of the statute does not contain a “clear indication” that Congress meant for the law to reach beyond the borders of the United States. Moreover, the court rejected the magistrate judge’s interpretation of the legislative history, claiming that the selections relied upon by the district court were mere “excerpts” that do not address any question of international reach. The court also relied on Congress’s use of the word “warrant”

---

75. *Id.* at 473.
76. *Id.* at 474.
77. *See Microsoft v. U.S.*, 829 F.3d at 211.
78. *Id.* at 213.
as a term of art, complete with the limitations that are traditionally inherent in that term.\textsuperscript{79} It found that the “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.”\textsuperscript{80} This means that compelling a private party to assist in obtaining information, such as by accessing data on its own servers, makes that action a search to which the Fourth Amendment’s warrant clause fully applies.\textsuperscript{81}

The Second Circuit appears to have the better of this argument. First, statutes that have been found to overcome the presumption of extraterritoriality all include clear language showing that the law was intended to apply outside the borders of the United States.\textsuperscript{82} No such language is present in the SCA. Additionally, because the SCA allows state courts to issue SCA warrants, it seems “particularly unlikely” that Congress would grant state courts such “authority without at least ‘address[ing] the subject of conflicts with foreign laws and procedures.’”\textsuperscript{83} Given the potential conflicts that could erupt if individual states were interfering with a foreign sovereign’s borders, and the lack of uniformity that could result, it seems difficult to find anything approaching a clear congressional intent to expand the SCA beyond the territorial borders of the United States in the language of the statute. Finally, and perhaps most telling, the government generally concedes that the warrant provisions of the SCA were not intended to apply extraterritorially.\textsuperscript{84} In both \textit{Microsoft} and \textit{In re Search Warrant No. 16-960-M-01 to Google},\textsuperscript{85} the parties did not dispute the language of the statute, instead preferring to focus on whether the conduct at

\textsuperscript{79} Id. at 212-13.
\textsuperscript{80} Id. at 214.
\textsuperscript{81} Id. See also Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971) (indicating that a private party assisting the government in a search becomes an \textit{agent} of the government, thus subject to the requirements of the Constitution as if the government itself was conducting the search).
\textsuperscript{82} See, e.g., 18 U.S.C. § 2331(1)(C) (2012) (referring to acts that “occur primarily outside the territorial jurisdiction of the United States”); see also \textit{Microsoft v. U.S.}, 829 F.3d at 211 (citing United States v. Weingarten, 632 F.3d 60, 65 (2d Cir. 2011) (noting the Second Circuit concluded that § 2423(b) "criminalize[d] ‘travel in foreign commerce undertaken with the intent to commit sexual acts with minors’ that would violate United States law had the acts occurred in the jurisdiction of the United States").
\textsuperscript{83} \textit{Microsoft v. U.S.}, 829 F.3d at 211 (quoting Arabian Am. Oil Co., 499 U.S. at 256).
\textsuperscript{84} See id. at 210-11 (noting that the government conceded the SCA’s extraterritoriality at oral argument); see also \textit{In re Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, No. 2:16-mj-02197}, 2017 WL 3263351, at *4 (C.D. Cal. July 13, 2017).
issue was actually an extraterritorial application of the relevant statute.\footnote{86}{See Microsoft v. U.S., 829 F.3d at 209; In re Search Warrant No.16-960-M-01 to Google, 232 F. Supp. 3d 708, 717 (E.D. Pa. 2017).}

This may simply be an effect of the age of the SCA. When the SCA was enacted, there was not the same level of internet traffic travelling back and forth between countries.\footnote{87}{See Sophia Dastagir Vogt, The Digital Underworld: Combating Crime on the Dark Web in the Modern Era, 15 SANTA CLARA J. INT’L L. 104, 112 (2017); see also Under My Thumb: Governments Grapple With Law Enforcement in the Virtual World, ECONOMIST (Oct. 10, 2015), http://www.economist.com/news/international/21672204-governments-grapple-law-enforcement-virtual-world-under-my-thumb.}

Moreover, the sheer amount of information being saved and stored in online servers could not have been contemplated by Congress.\footnote{88}{See infra notes 129-133 and accompanying text.} But, even if true, the correct result is for Congress to amend the SCA, not for courts to try to update the statute through judicial decision making.\footnote{89}{See generally Gevurtz, supra note 67; see also Zheng v. Yahoo, Inc., No. C-08-1068, 2009 WL 4430297, at “4 (N.D. Cal. Dec. 2, 2009) (stating that a judicial role in enforcing or restricting extraterritorial application of a statute is only proper “[w]here Congress makes clear its intent that a statute is to apply outside the United States”).}

Having concluded that the SCA does not appear to facially overcome the presumption against extraterritoriality, this Article turns to the second step of the \textit{Morrison} framework: determining the focus of the SCA and whether the conduct at issue when an SCA warrant requires a provider to bring information back to the United States constitutes an extraterritorial application of that statute.

2. What is the Focus of the SCA?

In \textit{Morrison}, the United States Supreme Court found that the focus of a statute resolves a claim of extraterritoriality. As stated by Professor Franklin A. Gevurtz, “[i]f the event which is the focus of the statute occurs in this country, there is no extraterritoriality; if the event which is the focus of the statute occurs abroad, there is.”\footnote{90}{Gevurtz, supra note 67, at 366.} But this leaves open the question of how to determine that focus. Courts have relied on the plain language and meaning of the statute,\footnote{91}{See, e.g., Gottlieb v. Carnival Corp., 436 F.3d 335, 337 (2d Cir. 2006).} as well as a more holistic approach, examining the framework of a statute, its procedural aspects, and its legislative history.\footnote{92}{Cf. Morrison, 561 U.S. at 266-70; Loginovskaya v. Butratchenko, 764 F.3d 266, 272 (2d Cir. 2014).}

The Second Circuit found that the SCA’s purpose is to \textit{protect} user data; that is, it considered the focus of the SCA to be the customers’ privacy.\footnote{93}{Microsoft v. U.S., 829 F.3d at 220.} As an initial matter, the act that the SCA is part of has the
word “privacy” in its title—the Electronic Communications Privacy Act. Moreover, the provisions allowing access to protected data are exceptions to the general rule. The SCA “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.” The Court found that the use of the term warrant supported this reading. A warrant is a device that allows the government to breach standard privacy protections under the Fourth Amendment. Therefore, the provision at issue here is only tangentially related to the overarching purpose of the SCA, which is to protect the privacy of individuals’ electronic data.

But this is not the only plausible reading of the SCA. The government has consistently urged courts to find that disclosure, not privacy, is the hallmark of the SCA. Importantly for this type of argument, in Morrison and RJR Nabisco, Inc. v. European Community, the United States Supreme Court appeared to narrow its focus of a statute’s purpose to the specific conduct at issue, rather than looking at the statute more broadly. There, the Court found that “sale” was the focus of § 10B of the Securities Exchange Act, rather than fraud. There is nothing in the language or the broader statute, or specifically about § 10B itself that favors one over the other; as Professor Franklin Gevurtz has pointed out, “[t]he sale is the so-called focus of section 10B simply because it [was] the conduct which, according to the Court, Congress intended must occur . . . in order to trigger the statute.” Applying that type of test here, it would seem that disclosure should be considered the focus, because it is the need for disclosure that triggers the need for an SCA warrant.

Moreover, the privacy protections built into the SCA are only against unauthorized disclosure. Yet the SCA warrant specifically authorizes federal agents to compel such disclosure. There is nothing in the SCA, or the ECPA generally, that prevents providers from

---

95. In re Google Inc. Cookie Placement Consumer Privacy Litig., 806 F.3d 125, 145 (3d Cir. 2015) (internal quotation omitted).
96. See, e.g., In re Search Warrant, 232 F. Supp. 3d at 717.
100. Gevurtz, supra note 67, at 370.
101. See 18 U.S.C. § 2702(a) (“[A] person or entity providing an electronic communication service to the public shall not knowingly divulge to any person or entity the contents of a communication while in electronic storage by that service.”).
making authorized disclosures of subscribers’ data. To the extent any such privacy concerns are implicated, they should be adequately protected by the requirements of obtaining a warrant. Therefore, when examining the specific focus of the statute at question in these types of cases, it seems that the relevant focus is on when protected data may be disclosed, not when it must be kept private.

3. Does an SCA Disclosure Occur Extraterritorially?

Accepting for purposes of the argument that privacy is the focus of the SCA, the final question is whether the conduct at issue was an extraterritorial application of the statute, or did it occur domestically.103

In Microsoft, the magistrate judge ultimately upheld the validity of the warrant, focusing more on the process of how the SCA warrant worked in obtaining electronic information than with the actual location of the information.104 Unlike a traditional warrant, which requires U.S. government agents to physically enter the premises and seize the authorized documents,105 the SCA order is “executed like a subpoena in that it is served on the ISP in possession of the information and does not involve government agents entering the premises of the ISP to search its servers and seize the email account in question.”106 U.S. government agents would not have to travel to Ireland and infiltrate the Microsoft server base to seize the e-mails associated with the suspected user. Instead, they could use any Microsoft computer within the United States, if the computer has the proper user information and e-mail retrieval software to view the pertinent stored information.107 Thus, the magistrate judge concluded that the SCA warrant operates domestically, requiring the provider to only disclose information within the borders of the United States. In short, this dispute boils down to a question of control, not a question of loca-

---

103. This leads to an initially strange question of how privacy can be considered conduct at all. However, the United States Supreme Court has explained that the presumption applies “regardless of whether the statute in question [1] regulates conduct, [2] affords relief, or [3] merely confers jurisdiction.” RJR Nabisco, 136 S. Ct. at 2101; see also Kiobel v. Royal Dutch Petrol. Co., 133 S. Ct. 1659, 1664 (2013) (noting that the statute in question, “does not directly regulate conduct or relief. It instead allows federal courts to recognize certain causes of action”).

104. See Magistrate Judge’s Decision, 15 F. Supp. 3d at 471-77.

105. See Fed. R. Crim. P. 41 (outlining the procedures of a traditional criminal warrant).

106. Magistrate Judge’s Decision, 15 F. Supp. 3d at 472 (alteration added).

107. See id. at 468 (stating that Microsoft’s Global Criminal Compliance (“GCC”) team members can use “a database program or ‘tool’ to collect the data” stored in Dublin, Ireland, by initially using the “tool” to locate where the target account is stored and then to collect the information or data associated with that account remotely from the server, wherever it is located).
tion.\textsuperscript{108} So long as the providers have control over the user’s e-mails and could access them within the United States, there is no reason why they should be precluded from disclosing the e-mails in connection with a domestic criminal investigation.

This argument relies primarily on a 1984 decision from the United States Court of Appeals for the Eleventh Circuit, commonly known as the “\textit{Bank of Nova Scotia Doctrine}” (\textit{“BNS Doctrine”}).\textsuperscript{109} The BNS Doctrine recognizes that a grand jury subpoena could be used to “compel a company subject to U.S. jurisdiction to produce evidence stored outside the United States if the evidence is within the company’s possession, custody, or control.”\textsuperscript{110} Further, because the BNS Doctrine was developed prior to the enactment of the SCA, Congress should be presumed to be aware of the existing case law and would have drafted the SCA to conform with the then-contemporary (and recent) BNS Doctrine, absent explicit language to the contrary.\textsuperscript{111}

The United States District Court for the Eastern District of Pennsylvania, examining a case with very similar circumstances, also determined that there could be no search or seizure abroad, because there is no “meaningful interference with the account holder’s possessory interest.”\textsuperscript{112} Nothing prevents the customer from continuing to access his or her information, and providers generally admit that they regularly transfer data from one data center to another without the customer’s knowledge.\textsuperscript{113} To the extent that this may constitute some type of abstract interference, such an interference is only de minimis and temporary.\textsuperscript{114} Courts have held that photocopying documents or taking photographs of evidence does not constitute a seizure either

\begin{itemize}
  \item \textsuperscript{108} See id. at 472 (“It has long been the law that a subpoena requires the recipient to produce information in its possession, custody, or control regardless of the location of that information.”).
  \item \textsuperscript{109} See \textit{Bank of Nova Scotia}, 740 F.2d at 817.
  \item \textsuperscript{110} See id. This doctrine, and the potential effect the \textit{Microsoft} case had upon it is discussed in detail infra Part III.B.
  \item \textsuperscript{111} See Magistrate Judge’s Decision, 15 F. Supp. 3d at 466; see also Jan. P. Levine, \textit{Feds Pose Privacy Risk by Grabbing Overseas ISP Emails}, Law360 (Sept. 8, 2014, 10:27 AM), https://www.law360.com/articles/574533/feds-pose-privacy-risk-by-grabbing-overseas-isp-emails (arguing that the district court’s interpretation is weak because of the apparent conflict regarding the reach of the BNS Doctrine, including whether the BNS Doctrine applies to warrants, a company’s business records, or also extends to its customers as well).
  \item \textsuperscript{112} See \textit{In re Search Warrant No.16-960-M-01} to Google, 232 F. Supp. 3d 708, 720 (E.D. Pa. 2017).
  \item \textsuperscript{113} See, e.g., \textit{In re Search Warrant}, 232 F. Supp. 3d at 720 (noting that Google regularly transfers customer data from one data center to another without informing the customer).
  \item \textsuperscript{114} Courts have recognized that de minimis interference with a person’s possessions is not sufficient to constitute a seizure under the Fourth Amendment. See United States v. Menon, 24 F.3d 550, 559-60 (3d Cir. 1994); cf. Arizona v. Hicks, 480 U.S. 321
\end{itemize}
because it does not deprive the owner of access to his or her property.115 It is difficult to distinguish how printing out copies of emails, when it does not prevent a customer from accessing them, using his or her account, or otherwise limits his or her own access to the information, should be considered any different. Therefore, any relevant disclosures only take place once the provider decides to comply with the SCA warrant, and give the information to the government. Because that occurs in the United States, there is no extraterritorial application.

The Second Circuit rejected this type of argument. According to the panel decision, the action sought by the government in its case—that Microsoft retrieve data located in Ireland—was extraterritorial and thus outside the scope of the SCA warrant authority.116 The Second Circuit disagreed with the lower courts that the relevant actions were taking place within the United States because providers, when accessing their datacenters overseas at the order of the government, are acting as agents of the U.S. government.117 Whether the information was being disclosed or not, the only reason for accessing the datacenter at that time was because the U.S. government requested it. Any interference through U.S. legal process, therefore, must constitute a search or seizure, and implicates both the presumption against extraterritoriality and the Fourth Amendment. Because this initial access is the relevant conduct being examined, the location of the data must be the key determinant to assessing whether the SCA warrant is being applied extraterritorially.

It should be noted that all of the judges dissenting from the denial of rehearing en banc disagreed with the panel on this point. These judges pointed out that the specific focus of the provision at issue here, § 2703, is on when a provider may disclose the information in its control, not on when such information is accessed.118 Judge Cabranes noted that mere access of a provider to information within its control does not invade a user’s privacy unless the provider divulges the communications to someone else.119 Judge Raggi similarly emphasized

---

115. *See* United States v. Mancari, 463 F.3d 590, 596 (7th Cir. 2006) (stating that photographing money was not an unreasonable seizure); Bills v. Aseltine, 958 F.2d 697, 707 (6th Cir. 1992); United States v. Thomas, 613 F.2d 787, 794 (10th Cir. 1980).


118. *See In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation*, 855 F.3d 53, 60-76 (2d Cir. 2017) (en banc) (Jacobs, Cabranes, Raggi, and Droney, JJ., dissenting).

119. *Id.* at 67-68 (Cabranes, J., dissenting).
that a § 2703 warrant “is executed with respect to . . . the person ordered to divulge materials in his possession,” not with respect to a place, and thus operates domestically when such a person is “within United States territory and subject to the court’s jurisdiction.” 120 Indeed, that has become a major crux of the government’s argument in its petition for certiorari to the United States Supreme Court, that a provider’s disclosure of information to the government is a “domestic, not extraterritorial, application” of the statute. 121

Additionally, the Second Circuit rejected the magistrate judge’s claim that an SCA warrant is a hybrid legal process, combining the law of warrants and subpoenas. It held that warrants and subpoenas are “distinct legal instruments” and there is no basis to infer that Congress wanted one term to mean the other. 122 The court also distinguished those cases, such as Bank of Nova Scotia, which allowed subpoenas to reach information held outside the United States. The court pointed out that Microsoft is merely a “caretaker” for the information, and that the customer or subscriber retained a protectable privacy interest in his or her emails, contrary to the business records that the BNS Doctrine could reach. 123 It clarified that because of these distinctions, its holding in this case was limited to SCA warrants, and left for another day the question of the constitutionality of the subpoena and court order provisions. 124

The limitations imposed by this type of ruling are extreme. Pursuant to this ruling, U.S. courts cannot issue any legal instrument that can reach data that is being stored overseas. When the U.S. government wants access to such data, it must make a diplomatic request, through a Mutual Legal Assistance Treaty (“MLAT”) or similar device, to the host country. Even though this raises significant practical problems for law enforcement because of the cumbersome nature of MLATs, because of the “the powerful clues in the text of the [SCA],

120. Id. at 70 (Raggi, J., dissenting). Judge Raggi opined:

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. It need only touch some keys in Redmond, Washington. If I can access my emails from my phone, then in an important sense my emails are in my pocket, notwithstanding where my provider keeps its servers.

Id. See also id. at 61 (Jacobs, J., dissenting).


122. Microsoft v. U.S., 829 F.3d at 214. The fact that the same statute uses both the term warrant and the term subpoena to signal differing levels of protection and to reach different levels of data is compelling evidence that there is a meaningful distinction between the two in the SCA. See 18 U.S.C. § 2703.

123. See Microsoft v. U.S., 829 F.3d at 215-16.

124. See id. at 218 (“Today, we need not determine the reach of the SCA’s subpoena provisions, because we are faced here only with the lawful reach of an SCA warrant.”).
its other aspects, legislative history, and use of the term of art ‘warrant,’ . . . lead [the court] to conclude that an SCA warrant may reach only data stored within United States boundaries.”125

III. THE IMPLICATIONS FOR THE SCA AND THE FOURTH AMENDMENT

Before analyzing the effect the ruling in this case may have, it is important to make clear that cases such as these are not “privacy” cases. The government has met the requirements of the Fourth Amendment’s strictest protections—appearing before a neutral magistrate judge, demonstrating probable cause, and reasonably tailoring its request to information relevant to an ongoing criminal investigation—to obtain an SCA warrant. Thus, while there are certainly privacy implications in the government seeking access to a person’s emails, in this case, the real concern the court was addressing was sovereignty.126 This Article, however, focuses on the rationale employed by the United States Court of Appeals for the Second Circuit to find that the presumption against extraterritoriality applies to SCA warrants and how such a rationale could impact other privacy doctrines under the Fourth Amendment. This section first assesses the influence this decision will have on challenges to the subpoena and court order provisions of the SCA. It then expands to wider doctrines, considering whether this decision may be used to further limit, or even overrule, the BNS Doctrine and the third-party doctrine.

A. THE SUBPOENA AND COURT ORDER PROVISIONS OF THE SCA

The Second Circuit ostensibly limited its decision to the SCA warrant provision.127 Yet, its conclusion—that a company accessing its own servers at the request of the government constitutes a search—begs a question: why would the use of administrative subpoenas or court orders to acquire the same information through the same action be any different? It is difficult to imagine any argument that the use of subpoenas or court orders do not interfere with the sovereign interest of the foreign state in any lesser manner.

Perhaps most intuitively, the provision of the SCA that allows the use of subpoenas or court orders to access the content of emails that are over 180 days old makes little sense with respect to this decision and common practices today. Emails are regularly saved and accessed

125. Id. at 221.
126. See Daskal, supra note 10, at 488 n.53, as well as the accompanying text; see also Webinar, supra note 11, as well as the accompanying text.
127. See Microsoft v. U.S., 829 F.3d at 121, as well as the text at supra note 124.
more than six months later.128 Indeed, some government regulations specify that certain record types must be kept for years, including up to the “life of the enterprise.”129 Yet this statute arguably creates a distinction in the level of protection granted to these emails by allowing a showing of only reasonable suspicion, or in the case of a subpoena, almost no showing at all.130

Certainly, if the old emails were stored overseas, a plaintiff would cite Microsoft v. United States131 to quash such a subpoena or order. The same international interests are implicated, and the order is asking the company to do the same thing a warrant would ask it to do. This is the easy case. But even if the content were stored within the United States, a plaintiff should be able to quash the order. If the Second Circuit is correct that the ISP becomes the agent of the U.S. government, and that accessing their own servers to produce the information is a search under the Fourth Amendment, then it should not matter where the data is located. By using a vehicle less stringent than a warrant to access the data, the government is arguably violating the Fourth Amendment. This is true no matter where the data is located. Thus, the conclusion reached by the Second Circuit may undermine the ability of an SCA subpoena or court order to obtain a customer’s email contents.

The requirement that the subscriber be notified in order to obtain content through a subpoena or court order does not save these provisions. The government could argue that, because the customer generally must be informed of requests for his or her email content, the customer can object on his or her own when he or she is formally charged.132 In other words, because the customers are informed about what information is being sought, they have implicitly consented to the disclosure. Yet, that would create further issues for the warrant requirement. First, simply providing notice is not the same as asking for permission for the search.133 It is hard to imagine anyone agreeing that law enforcement can search a home by simply telling the resi-

129. See Contoural, Inc., How Long Should Email Be Saved? 7 (2007), http://www.umiacs.umd.edu/~oard/teaching/708x/spring09/41.pdf; see also Green, supra note 5, at 190-91 (discussing the difference between use of email in the 1980s and today).
131. 829 F.3d 197 (2d Cir. 2016).
133. Cf. United States v. Most, 876 F.2d 191, 199 (D.C. Cir. 1989) (stating that store employees’ cooperation did not amount to implied consent to search the defendant’s bag when there was no evidence that officers requested permission before search).
dent what they were looking for without waiting for any specific response. Further, the United States Supreme Court has recognized that, when the government seeks to justify a search by consent, it is the government that bears the burden of proving both the existence of consent, and that such consent was freely and voluntarily given.134 Merely showing that the customer received notice is simply not sufficient to carry that burden.

Second, the government can avoid this notice requirement with relative ease. Under § 2705, the government may seek a nondisclosure order, preventing the provider from informing the customer that his or her information is being sought, if the government can demonstrate a “reason to believe” that the notification will create an “adverse result” on the criminal investigation.135 For example, courts have held that this burden is met by showing that the ISP has a “policy and practice” of notifying customers of subpoenas it receives.136 In many cases, the provider does not even have the opportunity to contest the nondisclosure order because it is unlikely the provider will be able to offer pertinent information about whether such notification would create an “adverse result” as defined by the statute.137 This provision makes it far more likely that the government will attempt to forestall a customer’s notification, and compel disclosure without the customer’s consent, in violation of the Fourth Amendment.

The primary impact of this case on other provisions of the SCA will be for circumstances where the government seeks the content of a user’s emails through a subpoena or court order. However, when non-content data is sought, such as basic subscriber information or a list of contacts, the provisions may fare better. If the information is located within the United States, there is no argument a conflict of laws ex-

134. See Bumper v. North Carolina, 391 U.S. 543, 548-49 (1966); see also United States v. Jaras, 86 F.3d 383 (5th Cir. 1996); United States v. Gonzalez, 71 F.3d 819 (11th Cir. 1996); Patzner v. Burkett, 779 F.2d 1363, 1369 (8th Cir. 1985) (“Consent cannot be presumed from the absence of proof that a person resisted police authority or proof that the person merely acquiesced.”); State v. Kudron, 816 P.2d 567, 571 (Okla. Crim. App. 1991) (rejecting the claim “that silence in the face of a request to search or a defendant’s failure to expressly object to a search is evidence of consent”) (“The trier of fact should be slow in finding intentional and voluntary relinquishment of immunity from search without a warrant when from the evidence the matter is somewhat in doubt.”).

135. See 18 U.S.C. § 2705(a). Such disclosure, however, cannot be indefinite; the interest served by preventing disclosure is generally not sufficient to justify a permanent gag order. See In re Sealing and Non-Disclosure of Pen/Trap/2703(d) Orders, 562 F. Supp. 2d 876, 886-87 (S.D. Tex. 2008) (construing § 2705 to only allow time-limited nondisclosure orders to avoid constitutional infirmity).


ists. Similarly, courts have recognized that there is not a protectable privacy interest in so-called metadata. Yet this assumption is regularly being challenged in courts, and at least one Supreme Court Justice has expressed doubts about the viability of this argument in today’s digital society. Further, how should these subpoenas or court orders be enforced if the metadata is stored outside the United States? The next two subsections consider this question.

B. THE BANK OF NOVA SCOTIA DOCTRINE

Such a narrow rationale may also undermine the ability of subpoenas to reach any records that are held outside the United States. Consider a hypothetical that changes some of the circumstances of the Second Circuit case. If the government had been seeking only non-content data of the subscriber and had sought a court order rather than an SCA warrant, Microsoft presumably would not have challenged the request; that data was located within the United States. But what if that non-content data had been stored overseas? Would the subpoena still have the force of law to compel such disclosure, even of non-content data?

According to the BNS Doctrine, which “compel[s] a company subject to U.S. jurisdiction to produce evidence stored outside the United States if the evidence is within the company’s possession, custody, or control,” the subpoena power of the SCA should still reach that information. In that case, the United States Court of Appeals for the Eleventh Circuit ordered “the disclosure of records stored in the Bahamas and maintained by a Canadian bank with U.S. branches.” The requested records were banking records of certain citizens. The court compared the interests of the government to pursue criminal investigation with the interests of American citizens to have their bank records remain private. The court found that the interests of the U.S. government in pursuing a criminal investigation outweighed

138. See, e.g., United States v. Davis, 785 F.3d 498 (11th Cir. 2015) (en banc); see also In re United States for Historical Cell Site Data, 724 F.3d 600 (5th Cir. 2013).
140. See Microsoft v. United States, 829 F.3d 197, 200 (2d Cir. 2016), cert. granted, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017) (noting that the requested data was on a server in Ireland).
143. Id. at 820.
144. Id.
those of an individual’s right to privacy.\textsuperscript{145} The court focused on the fact that the bank at issue had chosen to reach out to the United States by virtue of opening branches in the country, and thus had subjected itself to the proper jurisdiction of the courts.\textsuperscript{146} Thus, if a provider is subject to the personal jurisdiction of the subpoena-issuing court, it cannot “resist the production of [subpoenaed] documents on the ground that the documents are located abroad.”\textsuperscript{147} The test for production of this type of information is “control, not location.”\textsuperscript{148} Under this test, an SCA subpoena or court order should still be able to reach a subscriber’s non-content data. Courts have recognized that individuals do not have a legitimate privacy interest in this type of information.\textsuperscript{149}

But the conclusion of the Second Circuit in \textit{Microsoft v. United States}\textsuperscript{150} changes this analysis. In addition to considering the interest of the U.S. government and the privacy interest of individuals, the court factored in the sovereign interests of the nation where the data is stored.\textsuperscript{151} That interest does not change whether the request is for content or non-content data. The actual data—the ones and zeros that make up electronic information—are handled in the same way. In the \textit{Microsoft} case example, the company reaches into its Dublin datacenter and removes whatever information is responsive to the United States’s request. The Irish government may not even know whether this is content of emails or simply basic subscriber or payment information. The interests identified by the \textit{Microsoft} court, and the interests considered when assessing the presumption against extraterritoriality, are necessarily implicated whenever a company attempts to pull information outside that country’s borders.\textsuperscript{152} Applying

\begin{itemize}
  \item \textsuperscript{145} See id. at 828 (citing United States v. Payner, 447 U.S. 727, 732 n.4 (1980)) ("The interest of American citizens in the privacy of their bank records is substantially reduced when balanced against the interests of their own government engaged in a criminal investigation since they are required to report those transactions to the United States pursuant to 31 U.S.C. § 1121 and 31 C.F.R. § 103.24 (1979).").
  \item \textsuperscript{146} See id.
  \item In re Marc Rich & Co., A.G., 707 F.2d 663, 667 (2d Cir. 1983).
  \item Id.
  \item \textsuperscript{149} See, e.g., Smith v. Maryland, 442 U.S. 735 (1979) (finding a customer has no legitimate expectation of privacy in a telephone company’s records of telephone numbers dialed by the customer); see also \textit{In re Application of the United States for an Order Pursuant to 18 U.S.C. 2703(c), 2703(d) Directing AT & T, Sprint/Nextel, T-Mobile, Metro PCS, Verizon Wireless, 42 F. Supp. 3d 511, 517 (S.D.N.Y. 2014) (collecting cases)).
  \item \textsuperscript{150} See \textit{Microsoft v. U.S.}, 829 F.3d 197 (2d Cir. 2016).
  \item \textsuperscript{151} See \textit{Microsoft v. U.S.}, 829 F.3d at 225 (Lynch, J., concurring) ("We live in a system of independent sovereign nations, in which other countries have their own ideas, sometimes at odds with ours, and their own legitimate interests.").
  \item \textsuperscript{152} Id. at 220-21; see also Morrison v. Nat’l Austl. Bank Ltd., 561 U.S. 247, 255 (2010) (balancing the competing interests of the United States and a foreign nation when applying the presumption against extraterritoriality).
\end{itemize}
these interests to the BNS Doctrine calculus suggests that the doctrine may not be able to survive application of the Second Circuit’s rationale, even if the only information being sought is non-content data.

Returning to the facts of the Microsoft case, the Second Circuit attempted to distinguish the applicability of the BNS doctrine by pointing out that it only applies to a company’s own business records, and not to information that it is holding as a “caretaker for another individual or entity. . . .”\textsuperscript{153} Therefore, the court argued, the data at issue in cases such as In re Marc Rich & Co.\textsuperscript{154} and Bank of Nova Scotia\textsuperscript{155} were distinct from the business records obtained in the Microsoft case.\textsuperscript{156}

This line, however, is not as bright as the Second Circuit believes. As the government argued before the district court, a subpoena has been used to obtain private documents that were in the control or custody of a third party. In United States v. Barr,\textsuperscript{157} a subpoena was found sufficient to obtain unopened mail from an answering service that held it.\textsuperscript{158} The court in Barr found that, absent proof that the government coerced the disclosure, a subpoena itself is sufficient to merely obtain the information.\textsuperscript{159} Similarly, in United States v. Horowitz,\textsuperscript{160} a subpoena was used to obtain a defendant’s private file cabinet that was being held by his accountant.\textsuperscript{161} The court in that case held that because the subpoena was specific in its request and would not “unduly interfere” with the business of the accountant, there was no Fourth Amendment right to object to the disclosure.\textsuperscript{162} It is also important to clarify that the subpoenas in both these cases were not sufficient to review the private documents; a search warrant was required in both cases to actually read or open the private papers obtained.\textsuperscript{163} It was central to both courts’ holding that the subpoena was only being used to obtain the documents.\textsuperscript{164} It is unclear why this power to obtain should be limited only to subpoenas, when warrants,

\textsuperscript{153} Microsoft v. U.S., 829 F.3d at 215.
\textsuperscript{154} 707 F.2d 663 (2d Cir. 1983).
\textsuperscript{155} 740 F.2d 817 (11th Cir. 1984).
\textsuperscript{156} Microsoft v. U.S., 829 F.3d at 215-16.
\textsuperscript{157} 605 F. Supp. 114 (S.D.N.Y. 1985).
\textsuperscript{159} Barr, 605 F. Supp. at 119.
\textsuperscript{160} 482 F.2d 72 (2d. Cir. 1978).
\textsuperscript{161} In re Grand Jury Subpoena Served Upon Simon Horowitz, 482 F.2d 72, 75-79 (2d Cir. 1973).
\textsuperscript{162} Horowitz, 482 F.2d at 80.
\textsuperscript{163} See id. at 78; Barr, 605 F. Supp. at 118.
\textsuperscript{164} See Transcript of Record at 22, In re Grand Jury Subpoena Served Upon Simon Horowitz, 482 F.2d 72 (2d Cir. 1973) (No. 73-1570) (clarifying that the central point of Horowitz was that the documents were in the control of a third party).
including an SCA warrant, are subjected to the more rigorous probable cause standard. The warrant respects the privacy interests of the individual whose records are being sought and are only enforceable against parties that are subject to the jurisdiction of the issuing court.

Given the competing interests that play out in these subpoena cases, it is perhaps unsurprising to see courts expressing doubt over the continued viability of the BNS Doctrine.\(^{165}\) It is troubling that jurisdiction over a party should give a U.S. court the power to order a violation of another country’s laws.\(^{166}\) Moreover, neither Barr nor Horowitz involved an extraterritorial application; the documents at issue in both cases were located within the United States. It is too early, then, to claim that the BNS Doctrine has been completely overruled, but combined with other considerations, these cases suggest that courts may be more receptive to challenges to orders compelling action that will take place outside the United States.

C. THE THIRD-PARTY DOCTRINE

The third-party doctrine provides that Fourth Amendment protection is relinquished for information disclosed to a third party.\(^{167}\) Courts have relied on the third-party doctrine to allow the government to obtain cell phone locational information, numbers dialed from those phones, and bank records of individuals.\(^{168}\) Particularly relevant to non-content data, the government would argue that the privacy interest in any information they are requesting has been forfeited because it has been voluntarily given over to a third-party, and there is no barrier to disclosure.\(^{169}\)

---

165. See, e.g., In re Sealed Case, 825 F.2d 494, 498-99 (D.C. Cir. 1987); see also United States v. First Nat’l Bank of Chi., 699 F.2d 341, 346 (7th Cir. 1983) (rejecting the premise that an IRS summons could compel a bank to disclose records held outside the United States without demonstrating that the bank did not make a good-faith effort to comply with the summons).

166. See In re Sealed Case, 825 F.2d at 498-99; cf. Geoffrey Sant, Court Ordered Law Breaking: U.S. Courts Increasingly Order the Violation of Foreign Laws, 81 Brook. L. Rev. 181, 238 (“The very idea of U.S. courts ordering entities to break the law should shock the conscience.”).


169. See Daskal, supra note 10, at 492. This doctrine does not address the extraterritorial concerns raised, but as previously noted, the Microsoft case does not necessarily address the privacy concerns given that the government obtained a warrant. Yet, these types of privacy concerns provide a constant undercurrent in the arguments made by counsel for both Microsoft and the government.
The third-party doctrine, however, was developed in an era that contemplated neither the complexity of the Internet nor how widely used the Internet would eventually become. There are difficulties in applying the third-party doctrine to these circumstances. First, individuals’ emails are not actually given to the provider. The emails are held in encrypted servers, and it could be argued that the company itself is never given permission or access to the actual contents of those emails. Further, even if those servers are accessed, it is generally by an automatic computer system, not an actual human. Some commentators have argued that without exposure to an actual person, the information or data should still be considered to be within the possession of the owner. Interestingly enough, it was this type of argument that convinced the magistrate judge in Microsoft v. United States that the request to access data in a datacenter in Ireland did “not implicate principles of extraterritoriality” because “no such exposure takes place until the information is reviewed in the United States, and, consequently, no extraterritorial search has occurred.”

The Second Circuit appears to have disagreed with this conclusion. By finding that the search occurs where the data is located, even if that means only access by a computer system, the Second Circuit has ostensibly expanded the amount of information that has been “disclosed” to a third party. While it is unlikely that any court would find that a private email or correspondence that has been electronically processed has sacrificed all Fourth Amendment protection, as more information becomes exchanged through messenger applications
and cell phones, less of that information may be protected. This also raises questions about the privacy interest applicable to pictures, emojis, “likes,” and other electronic information that is exchanged through cyberspace.

Such an expansion could lead to more challenges to the third-party doctrine. The third-party doctrine remains good law today, but continues to be subject to numerous criticisms. In a concurrence in United States v. Jones, Justice Sotomayor argued that, given the realities of our current digital world, and the prevalence of third-party service providers facilitating information exchanges, “it may be necessary to reconsider the premise that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties.” These questions only become more significant as more information may be inadvertently disclosed through innovation, and there are at least four Supreme Court justices interested in addressing the viability of the third-party doctrine.

IV. MOVING FORWARD WITH THE SCA

After the Magistrate Judge’s Decision, several legal scholars argued that upholding the SCA warrant under the current statutory structure would undermine the United States’s position in the world, and offend international comity. Putting aside the concerns about

---

177. See Zachary D. Clopton, Territoriality, Technology, and National Security, 83 U. Chi. L. Rev. 45, 50-51 (2016). Even banking apps that are downloadable now, and allow individuals to create budgets and track expenses on their own devices, but also sync with their online account, may be subject to disclosure because they are reviewable and viewable by the bank. See, e.g., Mobile Banking Features, M&T Bank, https://www.mtb.com/banking/online-mobile-services/mt-mobile-banking (last visited Nov. 3, 2017).

178. See Chin Lin, supra note 172, at 1120.

179. See ACLU v. Clapper, 785 F.3d 787, 822-23 (2d Cir. 2015).

180. See Kerr, supra note 173, at 563 (“The third-party doctrine is the Fourth Amendment rule scholars love to hate” and has been condemned as no less than “the Lochner of search and seizure law, widely criticized as profoundly misguided.”); see also Jane Bambauer, Other People’s Papers, 94 Tex. L. Rev. 205, 261 (2015) (“The third-party doctrine has become the Fourth Amendment’s supervillain. It puts no constitutional limits on dragnet data collection.”); Stephen E. Henderson, Beyond the (Current) Fourth Amendment: Protecting Third-Party Information, Third Parties, and the Rest of Us Too, 34 Pepp. L. Rev. 975 (2007) (noting criticism of the third-party doctrine and describing alternative approaches adopted by some states for privacy protection).


183. See Jones, 132 S. Ct. at 957.


185. See, e.g., Alexander Dugas Battey Jr., Note & Comment, A Step in the Wrong Direction: The Case for Restraining the Extraterritorial Application of the Stored Communications Act, 42 Rutgers Comp. & Tech. L.J. 262 (2016); Daskal, supra note 22; Ashley Decks, Checks and Balances from Abroad, 83 U. Chi. L. Rev. 65 (2016); Freder-
the impact the United States Court of Appeals for the Second Circuit’s decision may have on other doctrines, this Article now considers how the jurisdiction of SCA warrants should be determined. It first considers, and rejects, the Second Circuit’s conclusion that the location of the data should be determinative. Rather, the more normatively appropriate considerations should revolve around whether the provider is subject to the jurisdiction of U.S. courts, and whether the target of the investigation is a U.S. citizen or national.

A. Problems with Location of Data as Determinant

The Second Circuit summarily concluded that the location of the data was the overriding factor in finding that the search occurred extraterritorially.\textsuperscript{186} Consider the implications: pursuant to this ruling, the U.S. government has jurisdiction over data held within the U.S. territorial jurisdiction, whereas the Irish government controls access to data within the territory of Ireland. If the United States wants data located in Dublin, it now needs to make a diplomatic request for the data—just as the United States would demand if Irish law enforcement sought data held in the United States.\textsuperscript{187}

While this provides the most privacy protections, such an approach also raises concerning issues. First, it provides a strong incentive for data localization laws as a means of controlling government access to sought-after data.\textsuperscript{188} Companies could seek to evade the U.S. government’s reach simply by moving communications data elsewhere, and governments could mandate that they do so to retain control over that data.\textsuperscript{189} This has negative consequences for the innovative potential of the Internet and for privacy rights of both American and foreign-based users. Data localization mandates are likely to result in foreign governments being able to compel the production of data—including data of Americans—based on a much lower standard than what would apply if the data were sought by the United States.\textsuperscript{190} Further, although data does indeed have a physical loca-


\textsuperscript{187} See Webinar, supra note 11. The use of MLATs and other international treaties raise significant practical concerns, including lengthy delays in processing, and the limited availability. See supra note 71 and accompanying text.

\textsuperscript{188} See Daskal, supra note 10, at 488.

\textsuperscript{189} Companies are incentivized to comply with such strong-arm measures to keep foreign customers and businesses, which have been estimated to comprise nearly $180 billion. See Russell Hsiao, Note & Comment, Implications for the Future of Global Data Security and Privacy, 24 Cath. U. J.L. & Tech. 215, 215 (2015).

\textsuperscript{190} See Daskal, supra note 10, at 489.
tion at any given time, its very mobility creates problems for subjecting it to the control of a jurisdiction. Data can be stored in a single location for seconds at a time before moving around, it can be stored at multiple locations at a single time, or it can be divided and stored in multiple locations at once. A court would have to wade through many problems, and different courts could issue conflicting decisions about the jurisdiction of a single piece of data.

There is also the simple problem of when the location of the data should be determinative. Warrants are legal documents, enforceable at the time of issuance, although they still must be executed on the target. Federal Rule of Criminal Procedure 41(b)(2) allows a judge to issue a warrant for a “person or property” that is in the appropriate district, even if that person or property may be moved outside the relevant district before the warrant can be executed. It can certainly be imagined that the government will request a warrant for data at Time One, the provider then moves the data overseas at Time Two, and the warrant is served on the provider at Time Three. It is unlikely that the government will know, at the time of a request, where the actual data is located. For example, as Google admitted in its own recent challenge to an SCA warrant, “the location of the data could change from the time the Government applies for legal process to the time when the process is served.” The district court in that case recognized that such considerations could lead to absurd results.

On one hand, even if the government knew the data was in the United States when the warrant was issued, the warrant may be defeated because the presumption against extraterritoriality (and the Second Circuit’s decision) mandates that the government proceed

191. See Woods, supra note 22, at 756-59.
192. See Daskal, supra note 10, at 489. But see Woods, supra note 22, at 758-60 (arguing that these features do not pose difficulties in assessing the proper jurisdiction for data).
193. See Fed. R. Crim. P. 41; see also Miller v. United States ex rel. Hunt, 181 F.2d 363 (5th Cir. 1950).
194. See Fed. R. Crim. P. 41(b)(2); cf. United States v. Krueger, 809 F.3d 1109, 1112 n.3 (10th Cir. 2015) (explaining that a warrant under Fed. R. Crim. P. 41(b)(2) is only valid if the property was located within the district of the issuing magistrate judge at the time the warrant was issued).
195. The cynical view is that providers would do such a thing with the goal of preventing U.S. government access. However, it is also likely that such a decision would be made because the customer notified the company they were moving to the destination country, signed up for a separate or new account, or due to a technical issue the provider is attempting to resolve.
196. See Webinar, supra note 11.
through means of an MLAT or similar international process. Law enforcement abided by proper procedures and met the high standard to get the warrant, fully expecting it to reach the data in issue. Moreover, it would further undermine the power of the U.S. courts to place the interests of foreign countries over the legitimate exercise of U.S. legal process when that process was only ever intended to operate inside the country.

Conversely, it seems problematic to allow the government to overcome the presumption against extraterritoriality simply because of a coincidence of timing. The provider may have been transferring information to comply with the foreign countries laws. Nothing in this hypothetical scenario undermines the sovereign interest of the foreign state. Similarly, this problem may lead to further conflicts with that foreign law. Even if the provider was planning to move the data back to the United States at a predetermined date, knowing that the data is now to be provided to the government may conflict with data localization mandates that would not have otherwise been violated. This may create adverse incentives for both individuals and companies to keep data moving around or even located on “server farms at sea” to avoid ever becoming subject to a single country’s jurisdiction.

Relatedly, even if the amorphous nature of data is not an insurmountable problem, there is the practical problem of introducing a disinterested third party into answering basic legal questions, such as jurisdiction. A service provider has no real interest in the investigation being conducted, yet its business decision to store data in a specific location is now determinative upon what jurisdiction controls. An unscrupulous company could certainly exploit this control to bargain with certain customers who are trying to avoid being subject to a particular jurisdiction. Similarly, this type of decision risks coming

---


200. See Cox, supra note 2, at 34 (citing Magistrate Judge’s Decision, 15 F. Supp. 3d at 475).

201. See Microsoft v. United States, 829 F.3d 197, 198 (2d. Cir. 2016), cert. granted, No. 17-2, 2017 WL 2869958 (U.S. Oct. 16, 2017) (noting that Microsoft’s decision on where to store data is determined by its business interest in reducing network latency); see also Swire & Hemmings, supra note 22, at 8-10 (discussing the costs and revenues businesses can gain from exploiting data localization).

202. The email service Lavabit was promoted on the idea that it would never reveal its customers’ data to the government, even if subjected to subpoenas or warrants. See Ladar Levinson, Secrets, Lies, and Snowden’s Email, GUARDIAN (May 20, 2014), https://www.theguardian.com/commentisfree/2014/may/20/why-did-lavabit-shut-down-snowden-email. The service is now defunct, but if it had moved its datacenter across the Texas border to Mexico, it could have successfully argued that it was not required to submit to any U.S. legal process.
across as arbitrary. An individual user often has no idea, nor does he or she really care, where his or her data is being stored. Why, then, should government access to one’s data depend upon where the data happens to be stored—particularly if the user does not know and has no role in choosing that location?

Finally, relying on location of data may erode the privacy protections for electronic data that the SCA put in place in the first place. If the government can conclude that, by accessing a subscriber’s data outside the United States, it is conducting a search under the Fourth Amendment, the only requirement it must meet is reasonableness. The warrant requirement would not be applicable because either: (1) the individual is not a U.S. citizen or national, and thus not entitled to the full protections of the Fourth Amendment; or (2) a warrant would not be effective or enforceable outside the United States anyway. Thus the government could argue that whatever actions it took were merely reasonable in light of the circumstances facing it. For example, future treaties or MLAT process could be negotiated to facilitate access to information, in exchange for sacrificing some of the privacy protections granted to data located inside the United States. If the foreign nation agrees, any action the United States takes pursuant to that agreement is likely to be considered reasonable.

The government could also incentivize providers to comply with data requests and argue that a request to the holder of the information is the most reasonable action that it could take. Consider a situation in which the U.S. government is investigating email fraud and identity theft. The government approaches a provider to request the contents of emails of a specific customer. The provider claims that the information is stored outside the United States, and thus, no legal process can compel it to disclose that information. However, the government also shows that the suspect of the investigation has targeted the provider itself or other customers of its service. The provider very

203. See Daskal, supra note 22, at 365-77, 379-96 (making this argument in much more detail).

204. See United States v. Verdugo-Urquidez, 494 U.S. 259, 271, 275 (1990) (holding that the Fourth Amendment’s warrant requirement does not apply to a search of a non-resident alien’s residence outside the United States); see also In re Terrorist Bombings of U.S. Embassies in E. Afr., 552 F.3d 157 (2d Cir. 2008) (holding that a warrant was not required for the search of a U.S. citizen’s residence or cell phone located in Kenya, Africa).

205. Verdugo-Urquidez, 494 U.S. at 271.

206. See In re Terrorist Bombings, 552 F.3d at 163.

207. See Daskal, supra note 10, at 490-92 (discussing the difficulties the U.S. blocking provisions create in obtaining data from foreign nations).

208. See Green, supra note 5, at 198-200 (discussing privacy policies moving forward from the Microsoft decision).
well may conclude it is in its own interest to hand over that information, despite there being no formal compulsion. Should the subject of a search be a U.S. citizen, this could mean that his or her emails are being turned over to law enforcement without the benefit of judicial scrutiny or the requirement that the government demonstrate probable cause. At the very least, it could make the decision to bring the data back into the United States, and thus be subject to an SCA warrant.

B. NEW APPROACH FOR ASSESSING JURISDICTION OF SCA WARRANTS

The other likely candidates that could establish jurisdictional control over data would be either the identity or nationality of the target of the investigation or the location of the service provider. Both provide more stability than a test based on the location of data, but each comes with separate costs. This Subsection attempts to balance the competing interests between the two factors and proposes a new test that gives law enforcement the flexibility to effectively pursue investigations, while ensuring the ability of providers to protect their customers’ data and respect the myriad of potentially conflicting laws that an international company is often subject to.

1. Focusing on the Nationality of the Target

The most commonly-proposed solution is that the SCA should focus only on the identity of the target of the underlying investigation. Professor Jennifer Daskal has persuasively argued that this type of test is normatively appropriate—if the owner of the data being sought is a U.S. citizen or national, there are fewer concerns about conflicting with another country because the U.S. courts are only attempting to enforce U.S. laws against U.S. persons. The International Communications Privacy Act (“ICPA”), introduced in both houses of Congress, takes this type of approach. It allows law enforcement agencies to obtain from service providers the electronic communications of U.S. citizens and permanent residents regardless of where the individuals or communications are located, as long as officials first obtain a warrant. The bill also clears the way for law enforcement to use warrants to obtain electronic communications from service providers

210. See Daskal, supra note 10, at 490.
211. Id. at 485-92.
providers that are related to foreign nationals in situations either
where the foreign government does not have a law enforcement coop-
eration agreement with the United States or where a cooperating for-
egnment does not object to the disclosure.213

Yet, there are still difficulties with this approach, one practical
and one normative. As a practical critique, it is extremely difficult to
determine the nationality and location of the target prior to obtaining
the data being sought.214 Most governments simply will not have that
information ahead of time.215 Even if providers were mandated to
verify the IP address of the subscriber, such proxy methods do not re-
ally address the concerns raised here. IP masking technologies and
spoofing software exist make it relatively easy to mask a user’s actual
location.216 Even if the IP is accurate, that only reflects a person’s
location for the instant that he or she set up his or her account; it is
not an accurate reflection of a person’s nationality or status. Put sim-
ply, “any presumption, whether based on IP address or something
else, will yield both false positives and false negatives.”217

Others argue that a jurisdictional test that focuses on nationality
and location is “NIMBY-like” in that it carves out protections for a
nation’s own citizens, legal permanent residents, and denizens, but
permits third-party nationals’ data to be collected based on the (pre-
sumably) lower standards applied by requesting foreign govern-
ments.218 This critique is analogous to the concern about the so-called
“elimination” of the probable cause standard. It is premised on the
idea that the United States, in reserving the probable cause standard
for U.S. citizens, legal permanent residents, and persons located in
the United States, is leaving third-party nationals out to dry, subject
to the whims of foreign government requesters. Conversely, one De-
partment of Justice representative has argued, albeit in an unofficial
capacity, that an approach focusing on a target’s nationality, such as
that proposed by the ICPA, lowers the protections for U.S. citizen’s

213. See id.
214. See Krishnamurthy, supra note 22, at 12 (noting the practical difficulties with
such an approach).
215. Id.
216. See Drew Prindle, How to Be Anonymous Online, DIGITAL TRENDS (May 16,
217. Daskal, supra note 10, at 498.
218. See Albert Gidari, MLAT Reform and the 80 Percent Solution, JUST SECURITY
Under Gidari’s approach, expedited access to U.S.-held data would be permitted only in
the very narrow set of cases where there is a finding of dual criminality and all parties
to the crime (including witnesses) are within the territorial jurisdiction of the request-
ing state. But while this is an interesting approach, it is not likely to sufficiently satisfy
the foreign government interest in data located outside its borders. See Daskal, supra
note 10, at 480-90.
data, while increasing the protections for the data of foreign nationals, because of the increased procedural roadblocks it creates.\textsuperscript{219} Similarly, this does not address the situation in which the data being sought is located in a third-party country. For example, if the target is a Chinese citizen, but the data is in Ireland, it is unclear what sovereign interest the Irish government has in protecting that data.\textsuperscript{220}

Thus, the focus on nationality results in an additional balancing test, one that can only likely be answered by Congress as the political branch best suited to evaluating these types of concerns. While this approach may be intuitively appealing, the practical difficulties it raises have no easy answer.

2. Focusing on the Location of the Service Provider

After the Second Circuit’s decision, most commentators have assumed that the location of the provider is no longer an important factor to consider. The court seemed to clearly reject this type of analysis.\textsuperscript{221} Yet, it may provide the most suitable starting place for an SCA investigation. If the provider is subject to the jurisdiction of U.S. courts, then a warrant issued to it, within the United States, should be enforceable no matter where the data happens to be located.

There is precedent for enforcing this type of jurisdictional control over the controller of data. States have a considerable interest in regulating the commercial activity that takes place on their soil, including transnational data storage and cloud computing services. For example, the U.S. government has the authority to dictate the activity of its citizen corporations abroad, including prohibiting the payment of bribes.\textsuperscript{222} Further, the “minimum contacts” test, articulated in \textit{International Shoe v. Washington},\textsuperscript{223} is regularly employed to assert jurisdiction over Internet companies.\textsuperscript{224} These companies have “reached out” to the country in which it operates, and thus should reasonably

\textsuperscript{219. See Webinar, supra note 11.}
\textsuperscript{220. See Davis, supra note 185, at 15 (questioning what interests a host country may have in pure data that is not connected to its own citizens).}
\textsuperscript{221. Microsoft v. United States, 829 F.3d 197, 220 (2d Cir. 2016), cert. granted, No. 17-2, 2017 WL 2869956 (U.S. Oct. 16, 2017).}
\textsuperscript{222. See Foreign Corrupt Practices Act of 1977 §§ 103(a), 104, 104A, 15 U.S.C. §§ 78dd-1-3 (2014). The only federal appellate case to examine the scope of the Foreign Corrupt Practices Act (“FCPA”) is United States v. Kay, 513 F.3d 432, 440-43 (5th Cir. 2007) (endorsing the SEC’s broad view that the FCPA covers not only payments made to foreign officials to obtain or retain business, but also any improper payments that facilitate general business activities).}
\textsuperscript{223. 326 U.S. 310 (1945).}
anticipate being hauled into court, or in the case of the SCA, subjected to a warrant.\footnote{See La Marca, supra note 170, at 998-99.}

This type of jurisdictional control, however, may seem too broad to many. For example, why should the data of a company like Viber, which primarily operates in Asia,\footnote{See About, VIBER, http://www.viber.com/en/about (last visited Nov. 12, 2016).} be vulnerable to U.S. law-enforcement requests simply because they opened a small branch in California? Similarly, if the data in question has no connection with the United States—it has not been sent from or received by a person in the United States, nor does it necessarily concern conduct taking place in the United States—a company may not reasonably expect to have to litigate the privacy of that data. This type of conflict can be resolved through application of later personal jurisdiction cases like \textit{Goodyear Dunlop Tires Operations, S.A. v. Brown}\footnote{564 U.S. 915 (2011).} and \textit{Daimler AG v. Bauman}.\footnote{134 S. Ct. 746 (2014).} Under these cases, the Court recognized and rejected the argument that the activities of a subsidiary in a forum state can create personal jurisdiction over the parent company.\footnote{Diamler AG v. Bauman, 134 S. Ct. 746, 760-61 (2014).} Continuous and systematic business activity alone was not sufficient for establishing general jurisdiction; rather, a corporation’s affiliations must be so substantial and of such a nature as to render it “essentially at home” in that state.\footnote{Daimler, 134 S. Ct. at 768. Such a test is also consistent with the Court’s similar rejection of the “stream-of-commerce” analysis. See \textit{Asahi Metal Indus. Co. v. Superior Ct. of Cal.}, 480 U.S. 102, 103-04 (1987).} Thus, personal jurisdiction is limited to only those companies that are headquartered or that have their “principal place of business” within the United States.\footnote{See Daimler, 134 S. Ct. at 761; see also Silberman & Simowitz, supra note 37, at 346-47 (arguing that \textit{Daimler} has substantially limited the number of companies subject to U.S. personal jurisdiction).} This requires more than just showing that a provider has “minimum contacts” with the United States, and may help justify a court in exercising such a broad power as compelling the provider to disclose another party’s data that it has in its possession.\footnote{See Daskal, supra note 10, at 499; Silberman & Simowitz, supra note 37, at 359-60.} Professor Daskal has posited, while not supporting such an approach, that this type of limitation also may resolve any conflict of laws issues that could arise from a company being subjected to multiple jurisdictions.\footnote{Daskal, supra note 10, at 499. It should be noted that this type of approach is also subject to manipulation. Companies could decide to simply shift their headquarters or place of incorporation out of the United States, while maintaining a primary business interest here. \textit{See id.} However, such a change could result in forfeiting other benefits of U.S. incorporation, such as tax benefits, regulatory security, and other busi-...
Moreover, applying a narrower approach to jurisdiction, particularly in the case of cloud data, makes sense. It protects businesses from being unfairly subjected to overly broad jurisdictional control when they have not “purposeful[ly] avail[ed]” themselves of the forum state.\footnote{234} In the case of foreign companies that offer services to U.S. residents, it is those residents that have chosen to purchase and use the service. The actions of customers should not, on their own, subject a company to U.S. government mandates.\footnote{235} There may be an argument that by using such a service, the person has expressly attempted to move data outside the United States and away from any control by the U.S. government.

This should not be the end of the inquiry, however. Even if a court has the power to issue such a warrant to a provider, this does not account for any international comity concerns or the potential conflict of laws that may arise. The provider should be able to quash the warrant by showing either that they are subject to an actual conflicting law in the country where the data is located, or that the target of the investigation is not a U.S. national.

First, if the provider can demonstrate that an order by the court would require them to violate another country’s laws, the courts are not the appropriate venue for that conflict to be decided. There is no valid reason why the laws of one country should supersede those of another.\footnote{236} Yet, there should be some proof that there is such a conflict. In the Microsoft v. United States\footnote{237} case, neither Microsoft nor Ireland, in its amicus brief, claimed that pulling the data at issue back into the United States would violate any of Ireland’s data protection laws.\footnote{238} Therefore, there was a question of what precisely Ireland’s interest was, since the target was not identified as an Irish citizen, and Ireland had no actual law preventing the data from being moved.


236. See Sant, supra note 166, at 184.

237. 829 F.3d 197 (2d Cir. 2016).

238. See Brief of Ireland as Amicus Curiae Supporting Appellants at 4, Microsoft v. U.S., 829 F.3d 197 (No. 14-2985); see also Webinar, supra note 11.}
The court proceeded to discuss international sovereignty without pointing to any actual violation of or conflict with it. In a more extreme example, Google was unable to identify even a single country the SCA warrant it opposed would conflict with for the basic reason that it did not know where the data would be located at any given time. “Before a court bars the Government from using a judicially approved search warrant to require disclosure of user data that constitute evidence of crimes, it would do well not to be controlled by possibilities and legal abstractions, but to focus instead on realities.”

This requirement also is supported under a conflict of laws analysis. The absence of a specific law, or even the presence of a law that would lead to the same or substantially similar outcome, is deemed to be a “false conflict.” That is, there is no real concern that a court is asking a provider to violate another country’s sovereignty when complying with the SCA warrant would not violate the other country’s laws. There would only be a problem for the U.S. courts if the law it seeks to enforce would be considered “arbitrary or fundamentally unfair” under the Due Process Clause. Courts have generally held this to mean that for a statute to be consistent with due process, “there must be a sufficient nexus between the defendant and the United States.” Here, that problem is resolved by the additional requirement that the target of an SCA warrant—meaning the owner of the account—is either a national of the United States, or that the criminal activity being targeted took place within the United States.

More abstractly, it could also be argued that a country’s law is determined not only by the positive law it enacts—the behavior it explicitly prohibits—but by the country’s silence as well. Behavior

239. *Microsoft v. U.S.*, 829 F.3d at 221. “Admittedly, we cannot be certain of the scope of the obligations that the laws of a foreign sovereign—and in particular, here, of Ireland or the E.U.—place on a service provider.” *Id.*

240. See *In re Search Warrant No.16-960-M-01 to Google*, 232 F. Supp. 3d 708, 724 (E.D. Pa. 2017); see also supra notes 180-181 and accompanying text.


242. Colangelo, *supra* note 67, at 1055; see also Phillips Petrol. Co. v. Shutts, 472 U.S. 797, 838 n.20 (1985) (Stevens, J., concurring) (“[F]alse conflict really means no conflict of laws. If the laws of both states relevant to the set of facts are the same, or would produce the same decision in the lawsuit, there is no real conflict between them.”).


244. See Colangelo, *supra* note 67, at 1103.

245. *United States v. Davis*, 905 F.2d 245, 248-49 (9th Cir. 1990) (internal citation omitted); see also United States v. Yousef, 327 F.3d 56, 111-12 (2d Cir. 2003).

246. See Ernest Knabel, *Actions on Foreign Judgments*, 6 Yale L.J. 71, 99 (1896) (citing Bank of August v. Earle, 13 Pet. 519, 589 (1839)) (“In the silence of any positive rule, affirming or denying or restraining the operation of foreign laws, courts of justice presume the tacit allowance of them by their own government.”).
that is not explicitly proscribed by a country should be presumed permitted. 247 Applying that theory here, if a country has not enacted a specific blocking law, or other data protection provision that restricts removing data for the purpose of providing it to a foreign government, then such action, even at the request of the foreign government, should not be seen to conflict with that country’s laws. 248 Now, the downside of this requirement is that it may lead to a proliferation of data blocking statutes, with countries enacting them purely to allow providers to refuse to comply with SCA warrants and subpoenas. 249 Yet, the risk that foreign countries will act to protect their data is not, in and of itself, a compelling reason for abandoning a workable solution.

Similarly, if the provider can demonstrate that the target is neither a U.S. national, nor a person with any sufficient connection to the United States, a court may not be the best place to resolve this conflict. In Zheng v. Yahoo, Inc., 250 a district court rejected an argument that the SCA should apply when the data at issue was located in China, the employees who would access the data were in China, and the disclosure would have taken place in China. 251 The court there concluded that the fact that Yahoo was headquartered in the United States was not sufficient to mandate disclosure or to make the subsidiary in China submit to U.S. jurisdiction. 252 Thus, this type of inquiry would provide a second level of restriction on top of the already limited jurisdictional test under Daimler; it would not be sufficient to show only that the company was headquartered here, but that the information at issue had a similarly strong nexus with the United States. Should the company show that all the relevant action would take place outside the United States, the important factors are perhaps better considered through congressional action or diplomatic means. 253 Certainly if the data being requested is stored in the home nation of the target, that country would have an increased interest in


248. This becomes more complicated with the current trend of international agreements between groups of countries, in that a specific country’s law may not prohibit certain action, but a multinational agreement does. See Daskal, supra note 10, at 492-95. These types of restrictions should also be considered adequate to quash an SCA warrant.

249. See Daskal, supra note 10, at 476-77 (discussing the current trends in cross-border data access).


252. Id. at *4.

253. See supra Part IV.B.1.
protecting its citizens.\textsuperscript{254} And from a purely economic standpoint, knowing that a provider is able to defeat such a warrant and protect the data of foreign citizens relatively easily may encourage those businesses to use U.S. companies.\textsuperscript{255}

One of the benefits of this test is that it places the burden on the party with the best access to relevant information—the provider. The provider, more than either the government or even the owner of the data, knows where the data is located, and how it moves.\textsuperscript{256} The provider is, or at least should be, familiar with the data protection laws in the countries in which it operates, thus making it more able to identify an actual conflict between the laws of the requesting country and the laws of the host country. The provider’s information may not be completely accurate,\textsuperscript{257} but it at least provides some standard for a court to be able to balance the interests of each party. This does not remove or lessen any burden from the government; a neutral magistrate judge must still find that there is probable cause to believe that the requested data is material and relevant to an ongoing criminal investigation before the provider is required to make any response.\textsuperscript{258}

Critics argue that this may place too much of a burden on U.S. companies, making them less competitive in the international cloud-computing market.\textsuperscript{259} However, companies that wish to operate in the United States are already subject to increased burdens on their operations. They must comply with additional reporting requirements, securities regulations, limitations on their conduct abroad, and even human rights requirements that are not present in other countries.\textsuperscript{260} This type of burden is simply part of conducting business within the United States, and having access to the market here. Moreover, there are also a number of additional benefits that follow from being a U.S. company.\textsuperscript{261} Balancing these rewards with the responsibility of complying with SCA requests is all a part of carrying

\begin{footnotesize}
254. See Microsoft v. U.S., 829 F.3d at 220-21; Schultheis, supra note 141, at 671.
255. Cf. Schultheis, supra note 141, at 670-73 (arguing that forcing U.S. companies to give over data without any substantial means of combating the requests poses problems for U.S. competitiveness in the area of cloud-computing).
257. See supra notes 196-198 and accompanying text.
260. See, e.g., 15 U.S.C. §§ 78dd-1-3 (limiting how U.S. companies can conduct business involving foreign officials); William R. Rohrlich, SEC Regulations & Compliance, Considerations in Light of Recent Developments, ASVPATORE, March 2016, at 4-8 (discussing SEC compliance requirements on United States companies as opposed to foreign companies).
261. See Rohrlich, supra note 260.
\end{footnotesize}
the U.S. flag in your pocket. And for those companies that do not want to carry this increased burden, they may decide to move information or their operations outside of the United States. This is a risk any solution will carry. But again, other industries have done the same thing in response to U.S. regulatory requirements: for example, banks have shifted to the Cayman Islands or established Swiss locations to shield the identity of their account holders. These practical risks should not dissuade the formation of a test that respects both privacy and international concerns.

V. CONCLUSION

Courts have struggled to determine whether and how the SCA applies extraterritorially. The United States Court of Appeals for the Second Circuit’s holding in *Microsoft v. United States* means that SCA warrants cannot reach data that is being hosted outside the United States. It found that a government request that a service provider access its own servers to retrieve data makes the provider an agent of the government, and that act of access a search under the Fourth Amendment. It also concluded that the determinative factor to consider is the location of the data at the time the government requests the information from the provider. Yet, as discussed throughout this Article, these conclusions raise serious concerns for both the SCA itself, and other Fourth Amendment doctrines.

The purpose of this Article was not to provide clear answers to these questions, but rather to discuss how these competing interests interact, and identify some problematic conclusions that can be reached. As data has become increasingly global, the interest of law enforcement has followed. Requests for information are increasing as more and more information is transferred from the physical world to the digital one. A nuanced approach that allows law enforcement to carry out effective investigations, but still respects privacy and international sovereignty concerns, is necessary for companies to have a clear understanding of their obligation moving forward. Companies like Microsoft and Google should be applauded for trying to seek out clarification of their responsibilities, but a blanket ban restricting information outside the United States from ever being introduced, absent consent of the customer, is an unworkable solution.

---


263. 829 F.3d 197 (2d Cir. 2016).
As shown above, the consequences that result from the failure of courts to consider the uniqueness of data and this new internet age can be, at a minimum, bizarre. This situation demands increased attention, and likely action from Congress. The approach outlined above is but one way Congress, and the courts, can try to balance these competing concerns. This is a complex problem, and any solution must balance both the commitment of businesses to their customers’ privacy, and legitimate law enforcement need for access to data, while also promoting predictable jurisdictional boundaries.