Loyola of Los Angeles Law Review

Volume 50
Number 3 *Symposium & Developments in the Law*

Article 9

2017

Storage Wars: Analyzing the Territorial Limits of the SCA's Warrant Provision

Peter Liskanich
Loyola Law School, Los Angeles

Storage Wars: Analyzing the Territorial Limits of the SCA's Warrant Provision

Cover Page Footnote

J.D. Candidate, May 2018, Loyola Law School, Los Angeles. Thanks to the editors and staff of the Loyola of Los Angeles Law Review for their help in editing this Comment. Thanks, also, to Professor John Nockleby for his guidance. Lastly, thanks to my family and friends for their support throughout my law school career.

STORAGE WARS: ANALYZING THE TERRITORIAL LIMITS OF THE SCA'S WARRANT PROVISION

*Peter Liskanich**

I. INTRODUCTION

Technological innovation has historically forced the expansion of substantive law. For example, industrialization and the expansion of railroad systems led to major expansions in property law, tort law, and employment law, while the creation of the printing press prompted the development of copyright law.[1] But laws and regulations generally do not keep pace with the rate of technological change. Today, technology is evolving at a faster pace than ever before and legislators are struggling to keep up. As Professor Vivek Wadhwa points out, regulatory gaps exist, and as technology advances ever more rapidly, those gaps grow increasingly wider.[2]

The driving force behind innovation of the Digital Age has been the observed growth in computer processing power, which doubles nearly every two years.[3] The exponential growth in the capacity of computer processors has had a particularly profound effect on the expansion of the internet. According to data published by the World Bank, the percentage of the world's population with access to the internet has increased from less than two percent in 1996 to over forty-

* J.D. Candidate, May 2018, Loyola Law School, Los Angeles. Thanks to the editors and staff of the *Loyola of Los Angeles Law Review* for their help in editing this Comment. Thanks, also, to Professor John Nockleby for his guidance. Lastly, thanks to my family and friends for their support throughout my law school career.

1. Vivek Wadhwa, *Laws and Ethics Can't Keep Pace with Technology*, MIT TECH. REV. (Apr. 15, 2014), https://www.technologyreview.com/s/526401/laws-and-ethics-cant-keep-pace-with-technology.

2. *Id.*

3. David Frideman, *Does Technology Require New Law?*, 25 HARV. J. L. & PUB. POL'Y 71, 81 (2002).

three percent in 2015.[4] Today, more than three billion people use the internet and that number continues to grow exponentially.[5]

In 1986, under Title II of the larger Electronic Communication Privacy Act, Congress created the Stored Communications Act ("SCA" or the "Act") which "protects the privacy of the contents of files stored by service providers and of records held about the subscriber by service providers."[6] In 1986, the internet was still in its infancy; the drafters of the SCA had no way to foresee that multinational companies would be able to store vast amounts of digital content and easily transfer such information across borders at lightning speed.[7] Thirty years later, the internet has evolved from a collection of small networks into a global system for electronically transmitting communications, while the laws regulating the protection of those communications have remained the same.

This Comment will argue that the Second Circuit correctly applied the relevant provisions of the SCA to the facts of a recent case involving Microsoft—*Microsoft Corp. v. United States*—[8]but that there is no reasonable interpretation of the SCA as it currently stands that would adequately balance the legitimate needs of U.S. law enforcement and the privacy interests of U.S. citizens. Part II of this Comment will describe the facts of *Microsoft Corp.* Part III will examine the Second Circuit's application of the SCA. Part IV will analyze the merits of the Court's reasoning and discuss the practical implications of the Court's decision, including the consequences that might have followed from an opposite interpretation of the SCA. Finally, this Comment will discuss the merits of several proposed legislative and policy reforms.

II. STATEMENT OF THE CASE

Microsoft Corporation operates a "web-based e-mail service" known as Outlook.com.[9] In providing users with web-based access to e-mail accounts, Microsoft saves each user's e-mail information and

4. *Internet Users (Per 100 People)*, WORLD BANK GRP. (Nov. 3, 2016), http://data.worldbank.org/indicator/IT.NET.USER.P2.

5. Steve Dent, *There Are Now 3 Billion Internet Users, Mostly In Rich Countries*, ENGADGET (Nov. 25, 2014), https://www.engadget.com/2014/11/25/3-billion-internet-users.

6. Microsoft Corp. v. United States, 829 F.3d 197, 205 (2d Cir. 2016) (citation omitted).

7. *Id.* at 226 (Lynch, J., concurring).

8. 829 F.3d 197 (2d Cir. 2016).

9. *Id.* at 202 (majority opinion).

content on a network of servers located in massive datacenters operated by Microsoft and its subsidiaries.[10] Microsoft oversees more than one hundred datacenter facilities across more than forty countries and hosts more than 200 online services, used by over one billion customers and over twenty million businesses around the globe.[11] In an effort to reduce network latency, Microsoft typically stores a customer's e-mail information and content at a datacenter located near the physical locale identified by the user as its own when subscribing to the service.[12] However, Microsoft does not verify the accuracy of the user-provided information before its systems migrate the data according to company protocol.[13]

Once the user's content has been transferred to a foreign datacenter, Microsoft removes nearly all of the information associated with the account from its U.S.-based servers, retaining only basic account information and some non-content e-mail information in its U.S. facilities.[14] While Microsoft maintains that user data stored in Dublin is only accessible from the Dublin datacenter, Microsoft's database management program allows it to retrieve account data stored on any of its servers globally from its offices in the United States.[15]

In *Microsoft Corp.*, a magistrate judge for the Southern District of New York issued a Search and Seizure Warrant under section 2703 of the Stored Communications Act, directing Microsoft to seize and produce the contents of an e-mail account that it maintains for one of its customers.[16] The judge found probable cause to believe the account was being used in furtherance of narcotics trafficking.[17] However, due to jurisdictional limitations, Microsoft moved to quash the warrant to the extent that it required Microsoft to produce the contents of the customer's e-mail account stored on a server located in its Dublin datacenter.[18]

10. *Id.*
11. *Id.* at 202–03.
12. *Id.* at 202.
13. *Id.* at 203.
14. *Id.*
15. *Id.*
16. *Id.*
17. *Id.* at 204.
18. *Id.*

In support of its motion to quash, Microsoft referred to Congress's use of the term "warrant" to identify the instrument authorized under the Act, because "[w]arrants traditionally carry territorial limitations."[19] Microsoft cited 41(b) of the *Federal Rules of Criminal Procedure* to support its position that a court-issued warrant permits law enforcement agencies "to seize items at locations in the United States and in United States-controlled areas . . . but their authority generally does not extend further."[20] Conversely, the government attached little importance to the instrument's label. Instead, the government argued that the scope of a warrant under the SCA is more akin to that of a subpoena, which "requires the recipient to deliver records, physical objects, and other materials to the government no matter where those documents are located, so long as they are subject to the recipient's custody or control."[21]

The magistrate judge, affirmed by the district court, denied Microsoft's motion to quash and concluded that Microsoft was obligated to produce the customer's content, "wherever it might be stored."[22] The judge likened the instrument to a subpoena, rather than a traditional warrant, on the ground that an SCA warrant does not involve government officials entering the premises of the internet service provider to seize the relevant email account.[23] Accordingly, the magistrate judge determined that Congress intended the Act's warrant provisions to incorporate obligations similar to those associated with a subpoena and therefore held that Microsoft was required to produce information in its possession or under its control, irrespective of its location.[24]

However, on appeal, the Second Circuit reversed the district court's ruling and concluded that the SCA does not authorize a U.S. court to issue and enforce an SCA warrant against a United States-based service provider to obtain the contents of a customer's electronic communications stored on servers located abroad.[25]

19. *Id.* at 201.
20. *Id.* (citation omitted).
21. *Id.*
22. *Id.* at 204.
23. *Id.* (citation omitted).
24. *Id.*
25. *Id.* at 222.

III. REASONING OF THE COURT

The Second Circuit emphasized the strong presumption against extraterritorial application of U.S. laws, given that "the SCA is silent as to the reach of the statute as a whole and as to the reach of its warrant provisions in particular."[26] When interpreting the laws of Congress, courts presume that such laws are intended to "apply only within the territorial jurisdiction of the United States, unless a contrary intent clearly appears."[27] Here, the court followed the two-prong approach set forth in *Morrison v. National Australian Bank Ltd.*[28] to decide whether the presumption against extraterritoriality forbids the proposed application of the SCA.[29] First, the court must first look to the plain language of the statute to determine whether Congress intended it to have extraterritorial effect.[30] Second, if congressional intent is not found in the plain language of the statute, the court must rely on common canons of statutory construction to "identify[] the statute's focus," and determine whether, based on the facts, the challenged application is unlawfully "extraterritorial."[31]

A. Prong 1: The Plain Language of the SCA

In *Microsoft Corp.*, the Court first analyzed whether the plain language of the SCA contemplates extraterritorial application.[32] The Court readily determined that the SCA's provisions permitting a service provider's disclosure in response to a duly obtained warrant do not mention any extraterritorial application.[33] Moreover, the government was unable to point to any provision that even implicitly alluded to such application.[34]

Turning to the legal significance of the term "warrant," the court indicated that a legal term of art is to be interpreted "in accordance with [its] traditional legal meaning, unless the statute contains a persuasive indication that Congress intended otherwise."[35] Here, the court explained that "warrants and subpoenas are, and have long been,

26. *Id.* at 209.
27. *Id.* at 210 (citation omitted).
28. 561 U.S. 247 (2010).
29. *Microsoft Corp.*, 829 F.3d at 210 (citing *Morrison*, 561 U.S. at 255).
30. *Id.*
31. *Id.*
32. *Id.*
33. *Id.* at 211.
34. *Id.*
35. *Id.* at 212.

distinct legal instruments"[36] and that "[s]ection 2703 of the SCA recognizes this distinction and, unsurprisingly, uses the 'warrant' requirement to signal . . . a greater level of protection to priority stored communications, and 'subpoenas' to signal (and provide) a lesser level."[37] The court highlighted the fact that the statute explicitly refers to both instruments and yet it "does not use the terms interchangeably . . . [n]or does it use the word 'hybrid' to describe a Stored Communications Act warrant."[38] Thus, the court found no reasonable basis to infer that Congress intended a warrant under the SCA to function as a subpoena.[39]

B. Prong 2: Statutory Construction

The second prong of the approach, set forth in *Morrison*, requires a court to examine the "'territorial events or relationships' that are the 'focus' of the relevant statutory provision."[40] According to the court in *Morrison*, "[i]f the domestic contacts presented by the case fall within the 'focus' of the statutory provision or are 'the objects of the statute's solicitude,' then the application of the provision is not unlawfully extraterritorial."[41] Here, the Second Circuit relied on several common canons of statutory construction to support its conclusion that the "focus" of the SCA's warrant provision was to protect the privacy of stored communications.[42]

1. The Plain Meaning of the Text in the SCA

First, the court referred to the plain meaning of the text in the Act's warrant provision. The court pointed out that "[w]arrants under Section 2703 [are issued] under the *Federal Rules of Criminal Procedure*, whose Rule 41 is undergirded by the Constitution's protections of citizens' privacy against unlawful searches and seizures."[43] The court also called attention to the fact that the warrant language in section 2703 appears in a statute entitled the Electronic Communications Privacy Act, "suggesting privacy as a key

36. *Id.* at 214.
37. *Id.* (citing 18 U.S.C. § 2703(a), (b)(1)(A)).
38. *Id.* (citation omitted).
39. *Id.*
40. *Id.* at 216 (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 267 (2010)).
41. *Id.* (quoting *Morrison*, 561 U.S. at 267).
42. *Id.* at 217.
43. *Id.*

concern."[44] Thus, the court concluded, the language of both the SCA's warrant provision and the act as a whole suggest that the privacy of the stored communications is the "object of the statute's solicitude" and "the focus of its provisions."[45]

2. The Structure of the SCA

The Court also cited the statute's structure as a major indicator of the Act's focus on the need to protect users' privacy interests.[46] The court explained that the SCA primarily imposes obligations to protect the privacy of electronic communications and that "[d]isclosure is permitted only as an exception to those primary obligations and is subject to conditions imposed in [section] 2703."[47] Thus, although the SCA does prescribe means by which law enforcement may obtain access to user content, "it does so in the context of a primary emphasis on protecting user content," which the court described as the "object of the statute's solicitude."[48] The court mentioned in dicta that if the Act were truly focused on abetting law enforcement and disclosure, it would have instead created "a rebuttable presumption of law enforcement access to content premised on a minimal showing of legitimate interest."[49] But as the Court pointed out, "this is not what the Act does."[50] Thus, an examination of the Act's structure prompted the Court to conclude that the interest of law enforcement in compelling disclosure is secondary to the protection of users' privacy interests.

3. The Legislative History of the SCA

Finally, the court referred to the Act's legislative history, which indicated that when Congress passed the SCA as part of the broader Electronic Communications Privacy Act in 1986, its primary goal was

---

44. *Id*.

45. *Id.* (citing *Morrison*, 561 U.S. at 267) (internal quotations omitted).

46. *Id.* at 218 ("Section 2701 . . . protects the privacy interests of users in many aspects of their stored communications from intrusion by unauthorized third parties. Section 2702 generally prohibits providers from knowingly divulging the contents of a communication that is in electronic storage subject to certain enumerated exceptions. Section 2703 governs the circumstances in which information associated with stored communications may be disclosed to the government, creating the elaborate hierarchy of privacy protections that we have described.").

47. *Id*.

48. *Id.* at 217.

49. *Id*. at 218.

50. *Id*.

to protect user privacy in the context of new technology that required user interaction with service providers.[51] The legislative history also revealed that, with regard to governmental access, "Congress sought to ensure that the protections traditionally afforded by the *Fourth Amendment* extended to the electronic forum."[52] While the Court acknowledged that "Congress did not overlook law enforcement needs in formulating the statute," based on a report from the Senate Judiciary Committee, the Court found that those needs were not "the primary motivator[s] for the enactment."[53]

C. The Second Circuit's Conclusion

Having determined that the SCA's primary focus is on user privacy, the court concluded that the proposed execution of the warrant would constitute an unlawful extraterritorial application of the Act.[54] Because the content subject to the warrant is stored in, and would be seized from, the Dublin datacenter, and because Microsoft must necessarily interact with the Dublin datacenter in order to retrieve the information, the court determined that "the conduct that falls within the focus of the SCA would occur outside the United States."[55]

While the court acknowledged that the Act's focus on the customer's privacy might imply that the customer's actual location or citizenship would be relevant to the extraterritoriality analysis, it ultimately held that "the invasion of the customer's privacy takes place under the SCA where the customer's protected content is accessed," or, in this case, "where it is seized by Microsoft, acting as an agent of the government."[56] Thus, although Microsoft has the capacity to access information stored on any one of its servers located abroad, obtaining such information necessarily implicates the foreign subsidiary that manages the server and, consequently, the laws of the foreign country in which the server is located.[57] Therefore, the Second Circuit held the SCA warrant could not be used to lawfully compel

51. *Id.* at 201.
52. *Id.* at 219 (citing H.R. REP. NO. 99–647, at 19).
53. *Id.* at 219.
54. *Id.*
55. *Id.* at 220.
56. *Id.*
57. *Id.*

Microsoft to produce the contents of a customer's e-mail account stored exclusively in Ireland.[58]

IV. ANALYSIS OF THE SECOND CIRCUIT'S DECISION

A. Implications of the Second Circuit's Ruling

In response to the Second Circuit's decision, U.S. companies have already begun storing their information in data centers located outside the United States' territorial jurisdiction and beyond the reach of U.S. warrants.[59] As one commentator points out: "[d]ata center operations have been booming for years, but there's a new urgency in setting them up to help businesses establish a creative solution to privacy regulations."[60] Microsoft is not the only major internet service provider to make use of overseas data centers; companies such as Apple, Google, and Facebook already have substantial infrastructure in Ireland as well.[61] If Congress does not take action, more and more companies will begin taking advantage of the Second Circuit's decision.

By preventing SCA warrants from reaching data stored abroad, the court's decision functions as a substantial obstacle to the investigative efforts of law enforcement. As the magistrate judge who issued the warrant noted, it is quite easy for a wrongdoer to "mislead a service provider that has overseas storage facilities into storing content outside the United States."[62] Here, the Court condemned as unlawfully extraterritorial the government's attempt to compel a U.S.-based service provider to surrender information that is accessible from its U.S. facilities. Because the location of electronic documents is, "in important ways, merely virtual,"[63] such an outcome seems wholly incongruous. But despite the apparent illogicality of the Court's ruling, all things considered, the Second Circuit's decision was the optimal one.

---

58. *Id.* at 221.

59. Stephen Dockery, *Data Localization Takes Off as Regulation Uncertainty Continues*, WALL ST. J. (June 6, 2016), http://blogs.wsj.com/riskandcompliance/2016/06/06/data- localization -takes-off-as-regulation-uncertainty-continues.

60. *Id.*

61. Kate Conger, *Microsoft Triumphs in Warrant Case Against U.S. Government*, TECH CRUNCH (July 14, 2016), https://techcrunch.com/2016/07/14/microsoft-wins-second-circuit-warrant.

62. *Microsoft Corp.*, 829 F.3d at 221.

63. *Id.* at 229 (Lynch, J., concurring).

B. The Second Circuit Correctly Determined the Scope of the SCA's Warrant Provision

The Second Circuit correctly applied the Stored Communications Act in *Microsoft Corp.*; however, the statute is antiquated and does not present a workable framework for similar disputes in the future. Concurring in the judgment, Judge Gerald E. Lynch emphasized the need for congressional action to revise a badly outdated statute.[64] As Judge Lynch explained, "there are significant practical and policy limitations on the desirability of" "undertaking to regulate conduct that occurs beyond our borders."[65] Given the possibility of serious diplomatic repercussions, "the decision about whether and when to apply U.S. law to actions occurring abroad is a question that is left entirely to Congress."[66] This is because, as the majority noted, "Congress, rather than the courts, has the facilities necessary to make policy decisions in the delicate field of international relations."[67] Here, the Court was careful not to overstep its mandate by usurping the role of Congress and rightfully declined to give the warrant extraterritorial effect.

Although the government's position in this case seems logical as a matter of policy, an opposite outcome could have had serious negative implications. As Alan Raul and Kwaku Akowuah observed, "the Court was sensitive to issues of consistency and reciprocity between U.S. and foreign states."[68] Consistency and reciprocity are significant concerns within the context of the present case. Some experts worry that "if the U.S. insists on the power to force transfer of data to the U.S. from foreign servers, other countries—including those more aggressive than the U.S.—will insist on a reciprocal right. This could, of course, diminish the privacy rights of Americans."[69] Limiting law enforcement officials' access to information may make it more difficult for them to adequately protect citizens. However, given the vast amount of user data managed by internet service providers and the recent uptick in cyber-attacks on multinational

64. *Id.* at 222.
65. *Id.* at 225.
66. *Id.*
67. *Id.* at 210 (majority opinion) (citations omitted).
68. Alan Raul & Kwaku Akowuah, *2nd Cir. Microsoft Ruling: A Plea For Congressional Action*, LAW 360 (Aug. 1, 2016), https://advance.lexis.com/api/permalink/aa0bdaf4-c3bd-4c87-a786-a26308a8c8be/?context=1000516.
69. *Id.*

corporations, the interest in protecting user privacy is of the utmost importance and deserves serious consideration.

Moreover, as Judge Lynch acknowledged, there is no evidence that Congress has ever formally weighed the costs and benefits of authorizing court orders of the sort at issue in this case, primarily because "[t]he SCA became law at a time when there was no reason to do so."[70] This case highlights the profound tension between several conflicting interests: the legitimate needs of U.S. law enforcement to uphold the rule of law, the rights of foreign sovereigns to govern free from U.S. intervention, and the privacy interests of U.S. citizens who engage in on-line activity. Given the seriousness of the interests at stake, Congress should be the one to decide "whether the benefits of permitting subpoena-like orders of the kind issued here outweigh the costs of doing so."[71]

In short, the Second Circuit's decision should not be regarded as a "rational policy outcome, let alone celebrated as a milestone in protecting privacy."[72] Rather, the holding functions as "a plea for Congress to hash out the right policy balance. . . ,"[73] and symbolizes courts' unwillingness to make such decisions.

C. Possible Solutions

1. Data Localization

As a result of the Second Circuit's decision, Congress may feel compelled to pass strict data localization rules that would require technology companies to store user data in datacenters located within the United States' borders.[74] Under such rules, U.S.-based service providers would be unable to evade legitimate attempts by U.S. law enforcement to access customers' information simply by storing that information in overseas datacenters. However, the adoption of data localization rules—which effectively require data to be stored based on political considerations rather than technical efficiency—would "contribute to a trend of atomizing today's global Internet into

70. *Microsoft Corp.*, 829 F.3d at 231 (Lynch, J., concurring).
71. *Id.*
72. *Id.* at 233.
73. Raul, *supra* note 68.
74. Conger, *supra* note 61.

country-level networks."[75] Russia already imposes a strict data localization requirement, and in the last year alone more than twenty governments, including France and Brazil, have proposed similar legislation.[76] As one commentator points out, "[f]or many [governments], the stated reason has been not domestic monitoring, but rather protection against foreign government spying."[77] While localization rules may seem politically advantageous, internet experts have long objected to the adoption of data localization rules on a number of grounds.[78]

First, many experts have reservations as to whether localization rules actually afford users greater protection, since such laws effectively give local governments greater access to user data.[79] One commentator likened data localization to "a Balkanization or splintering of the Internet."[80] The same commentator argued that localization "makes the public at large less secure," because "[f]oreign countries may not respect the laws governing security, resulting in more access by state-sponsored surveillance or espionage."[81] As a result, a data localization requirement in the United States would "pose risks to political activists and human rights defenders by making their information more accessible to authorities."[82]

Second, critics argue that data localization laws would effectively act as barriers to trade by placing a substantial burden on global service providers in the form of increased costs.[83] For example, PayPal was forced to suspend its operations in Turkey after the Turkish government demanded that PayPal localize its infrastructure in order to continue operating.[84] Ramsey Homsany, general counsel of the file-

75. Katharine Kendrick, *Risky Business: Data Localization*, FORBES (Feb. 19, 2015, 5:08 PM), http://www.forbes.com/sites/realspin/2015/02/19/risky-business-data-localization/#155d6f538c8b.

76. Conger, *supra* note 61.

77. Kendrick, *supra* note 75.

78. *Id.*

79. *Id.*

80. Jocelyn Dong, *Silicon Valley Tech Execs: Surveillance Threatens Digital Economy*, PALO ALTO WEEKLY (Oct. 9, 2014), http://www.paloaltoonline.com/news/2014/10/09/tech-execs-surveillance-is-harming-digital-economy.

81. *Id.*

82. *See* Kendrick, *supra* note 75.

83. Dong, *supra* note 80.

84. Emre Peker, *PayPal to Exit Turkey After Regulator Denies Payments License*, WALL ST. J. (May 31, 2016), http://www.wsj.com/articles/paypal-to-exit-turkey-after-regulator-denies-payments-license-1464720574.

hosting service Dropbox, has said that the cost of setting up data centers across the globe would be prohibitively high—even for an established company like Dropbox.[85] According to Homsany, adoption of the data localization rules proposed by twenty foreign governments would dramatically restrict entrepreneurship and limit competition by making it "impossible" to start new technology companies.[86] Thus, adopting a data localization requirement would be imprudent because it would stifle innovation and economic growth.

Third, the fragmentation of the internet would inhibit the dissemination of data and lead to greater inefficiency. According to one article, "Colin Stretch, general counsel of Facebook, said that service to users would become less efficient, slower and less personalized because of companies' inability to take advantage of cloud-based storage that a well-networked Internet enables."[87] Richard Bennett, the vice-chair of the Institute of Electrical and Electronics Engineers Standards Association, explains that "[compliance] with data localization mandates not only requires more servers, it also requires more synchronization activity, which in turn requires more transmission capacity. This leads to a more complex Internet overall, which raises issues for Internet reliability."[88] Benett argues that no matter how "well-intentioned data localization mandates may be, over-broad restrictions on trans-border data flows are harmful to national security, destructive to the growth of the Internet, inconsistent with innovation, and bad for every user or firm who depends on the reliability of the Internet."[89] Therefore, Congress should resist the urge to implement strict data localization rules.

2. Strengthening Existing Mutual Legal Assistance Treaties

Some have also suggested enhancing the mutual legal assistance treaty process.[90] The term "mutual legal assistance treaty," or MLAT, refers to a category of treaties, generally bilateral, under which the United States and another country agree to use their respective legal

85. Dong, *supra* note 80. Dropbox provides data storage services to roughly three hundred million users, "[seventy percent] of whom are outside the United States." *Id.*

86. *Id.*

87. *Id.*

88. Richard Bennett, *Surge in Data Localization Laws Spells Trouble for Internet Users*, TECH POL'Y DAILY (May 10, 2016), http://www.techpolicydaily.com/internet/surge-in-data-localization-laws-spells-trouble-for-internet-users.

89. *Id.*

90. Raul, *supra* note 68.

processes to aid each other in the investigation and prosecution of criminal matters.[91] The Irish government reportedly backed Microsoft in the present case, arguing that "the U.S. could pursue the data through existing treaties with Ireland rather than trying to circumvent the country's sovereignty with a U.S.-based search warrant."[92] Thus, diplomatic engagement could potentially put the U.S. government in a position to sustain the interests of law enforcement and further international comity without sacrificing the privacy of millions of Americans.

While some foreign nations have been reluctant to cooperate with the United States in such matters ever since Edward Snowden shed light on the NSA's controversial surveillance activities,[93] the United States and the European Union have taken major steps towards implementing the "EU-U.S. Privacy Shield," which seeks to establish a safe framework for transatlantic data flows that will ensure greater protection for individuals and legal certainty for business.[94] However, a number of countries in Europe and around the world have recently implemented localization regulations, which some believe were intended to protect their citizens against U.S. espionage.[95] Thus, the U.S. must strive to engage foreign nations outside the EU-U.S. Privacy Shield and create an open dialogue; doing so will create opportunities for cooperation and potentially help restore trust in the U.S. government. If not, the U.S. government will be left with no formal means of garnering support to conduct law enforcement investigations in those countries with which it has not entered into an MLAT.[96] Still, the benefits of mutual legal assistance treaty reform are unlikely to be realized in the short run because the negotiation process often moves quite slowly.[97] Thus, the problem is one which also calls for legislative action.

91. Michael A. Rosenhouse, *Validity, Construction, and Application of Mutual Legal Assistance Treaties (MLATs)*, 79 A.L.R. Fed. 2d 375 (2013).

92. Conger, *supra* note 61.

93. Dong, *supra* note 80.

94. Press Release, European Comm'n, Statement by Vice-President Ansip and Commissioner Jourová on the Occasion of the Adoption by Member States of the EU-U.S. Privacy Shield (July 8, 2016), http://europa.eu/rapid/press-release_STATEMENT-16-2443_en.htm.

95. *Id.*

96. Microsoft Corp. v. United States, 829 F.3d 197, 221 (2d Cir. 2016) (citation omitted).

97. Raul, *supra* note 68.

3. Proposed Statutory Reform

While the U.S. must continue to pursue bilateral negotiations with foreign nations, Congress should seriously consider reforming the Stored Communications Act. Multinational service providers should not have the power to unlawfully obstruct the investigative efforts of the U.S. Justice Department and burden its ability to pursue matters related to domestic security. At the same time, the Justice Department must follow appropriate procedures that are substantively fair, "for it is procedure that marks . . . the difference between rule by law and rule by fiat."[98]

Pursuant to the government's argument in the present case, one possibility would be for Congress to submit legislation that would enable a duly authorized prosecutor to lawfully obtain a modified SCA warrant having extraterritorial effect.[99] Such an instrument would hypothetically compel a recipient to produce electronically stored information located on an overseas server that is under its control, even when the recipient is "merely a caretaker for another individual or entity and that individual, not the subpoena recipient, has a protectable privacy interest in the item."[100] But as one expert noted, "[i]f the U.S. government's position was validated by the Second Circuit, it would have forced multinational companies such as Microsoft to violate the laws of Ireland and potentially other countries in the future to comply with U.S. law."[101]

Therefore, if the modified SCA warrant does not comply with an existing MLAT treaty or multilateral agreement, the recipient of such an instrument may be forced to choose between violating a U.S. court order and being held in contempt, and violating the law of the foreign country in which it also does business. As one commentator notes, "[t]his would be an untenable position for not just Microsoft but any international company that has operations and customers in the U.S. and around the world."[102] On one hand, many multinational internet service providers would almost certainly comply with a U.S. court order, even if it meant violating the data export laws of a foreign

98. Wisconsin v. Constantineau, 400 U.S. 433, 436 (1971).

99. *Microsoft Corp.*, 829 F.3d at 215.

100. *Id.*

101. Bradley Shear, *Microsoft Search Warrant Case Is a Win for Privacy*, LAW 360 (July 22, 2016), https://advance.lexis.com/api/permalink/b6306d51-f226-4ba1-a854-0292f19ab11c/?context=1000516.

102. *Id.*

sovereign, in order to continue to avail themselves of access to U.S. markets and the protection of the U.S. rule of law. Nonetheless, it would be unwise as a matter of economic policy for Congress to put these businesses in such a position, because doing so would inhibit U.S. tech-startups from expanding their operations to foreign markets and might also deter foreign tech companies from expanding to the U.S.[103] Such a policy would erode the U.S. tax base for both foreign and domestic-source income. Therefore, any proposed legislative reform regarding the international reach of the SCA's warrant provision will necessarily require lawmakers to take into account the interests of other sovereign nations.

Many are hopeful that the Second Circuit's decision will inspire "cooperative efforts among government officials, service providers and privacy advocates" to solve the many issues surrounding international data storage and government access to electronically stored information.[104] While there have been a handful of unsuccessful attempts to modernize the SCA in the recent past, several members of Congress recently proposed legislation that would modernize the Electronic Communications Privacy Act (ECPA).[105]

In May, a bipartisan group of senators proposed the International Communications Privacy Act ("ICPA"), which would allow the use of domestic search warrants to retrieve electronic communications of U.S. citizens, permanent residents and some foreign nationals, wherever the individuals and content are located.[106] This sort of bright-line rule would provide clearer guidance to courts applying the law. Moreover, the proposed ICPA would "[r]eform the MLAT process by providing greater accessibility, transparency, and accountability."[107] Although the legislative process can be quite arduous, commentator Bradley Shear is confident that "[t]he U.S. as the birthplace of the Internet is perfectly situated to serve as a model

103. *Id.*

104. Raul, *supra* note 68.

105. Press Release, Congresswoman Suzan Delbe, Reps. DelBene, Marino Introduce International Communications Privacy Act (May 25, 2016), https://delbene.house.gov/media-center/press-releases/reps-delbene-marino-introduce-international-communications-privacy-act.

106. Randall Samborn, Esq. & Samantha Kruse, *The Government Isn't Winning the Crypto War but Is Anyone?*, 29 WESTLAW J. ENT. INDUS. 1, 2 (2016).

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

for the rest of the world on how to properly balance digital privacy with lawful access."[108] However, it is imperative that Congress act sooner than later.

V. CONCLUSION

The Microsoft case illustrates the challenges that courts face in applying an antiquated statute to contemporary issues concerning privacy and technology. Congress must act to implement a revised regulatory framework that is specifically tailored to the modern digital landscape. Strict data localization requirements are incongruous with achieving this end, because such policies fail to account for the complexities of today's global system of interdependent networks. Any attempt at legislative reform must take into account the needs and priorities of foreign sovereign nations and aim to streamline the existing MLAT process. Unless and until Congress replaces the Stored Communications Act, courts faced with situations like the one in the present case will inevitably reach similarly perverse results.

108. Shear, *supra* note 101.