NOTES

In re Warrant to Search a Certain Email Account: A Victory for Privacy in the Face of a New Technological World

I. OVERVIEW

The U.S. government issued a warrant pursuant to § 2703 of the Stored Communications Act (SCA) directing Microsoft to compel production of the contents of an email account.[1] A magistrate judge determined the government had established sufficient probable cause to believe the email account was used in the facilitation of narcotics trafficking.[2] The email account used Microsoft's Outlook.com web-based email service, where Microsoft facilitates email communication and stores the email contents on its network of servers.[3] Microsoft selects which server stores the customer's account contents using the user's self-reported country code, matching the user's represented physical location with a nearby server in order to reduce network delay.[4] Microsoft partially complied with the warrant by disclosing the requested information stored on servers in the United States.[5] However, Microsoft refused to produce contents that were stored on servers maintained in Dublin, Ireland, despite admitting it could collect the contents from its Dublin servers without physically going to Dublin.[6]

1. *In re* Warrant to Search a Certain E-Mail Account, 829 F.3d 197, 200 (2d Cir. 2016).
2. *Id.*
3. *See id.* at 202.
4. *Id.*
5. *See id.* at 204.
6. *Id.* at 203.

Microsoft moved to quash the warrant with respect to those contents stored on servers in Dublin, claiming that the SCA gives the government no authority to issue warrants on contents stored overseas.[7] The government argued the issued SCA warrant compelled disclosure, not production, of the user's contents, and the warrant would thus be lawfully applied domestically.[8] The magistrate judge denied Microsoft's motion.[9] He reasoned the SCA's "warrant" was actually a hybrid between a traditional warrant and a subpoena.[10] Further, he reasoned that the relevant location to consider when conducting an SCA "warrant" seizure analysis was "where the government would *review* the content (the United States)" as opposed to "the place of *storage* (Ireland)."[11] He rejected Microsoft's interpretation of the SCA's warrant provisions as inconsistent with the SCA's structure and legislative history and warned against the practical consequences of adopting such a position in the present technological world.[12] Microsoft appealed the magistrate judge's decision to the district court, which reviewed the case de novo and affirmed the magistrate judge's holding.[13] Microsoft timely appealed the district court's denial of its motion to quash to the Second Circuit.[14] Microsoft argued an SCA warrant is not subject to extraterritorial application.[15] The United States Court of Appeals for the Second Circuit *held* that the SCA's warrant provisions do not apply extraterritorially and that the enforcement of an SCA warrant to compel production of email content stored in a server located overseas would be unlawful extraterritorial application of the warrant. *In re Warrant to Search a Certain E-Mail Account*, 829 F.3d 197, 222 (2d Cir. 2016).

---

7. *Id.* at 204.

8. *See id.* at 201 (explaining the government's characterization of the dispute to be about "compelled disclosure").

9. *Id.* at 204.

10. *See id.* at 204, 214. The warrant is executed as a subpoena, according to the magistrate judge, because it "is executed by a service provider rather than a government law enforcement agent, and because it does not require the presence of an agent during its execution." *Id.* at 214.

11. *Id.* at 204.

12. *Id.*

13. *Id.*

14. *Id.*

15. *See id.* at 204, 209.

II. BACKGROUND

A. The Need To Protect Electronic Content

Due to a 1976 United States Supreme Court decision,[16] Congress recognized a need to expand legislation[17] to appropriately address the new reliance on electronic data.[18] In *United States v. Miller*, the Supreme Court held that bank records based on transactions with depositors constituted the bank's business records since the bank itself was a party to the transactions.[19] Thus, the records were not "private papers" protectable by the customer's Fourth Amendment rights.[20] Congress was concerned this decision brought into question whether a customer relying on electronic data maintained by a third party had any rights to assert in order to protect the privacy of their electronic records.[21]

Congress addressed this issue by passing the Electronic Communications Privacy Act (ECPA) in 1986.[22] Before Congress passed this act, the actions of private parties who controlled customers' electronic data was "largely unregulated and unrestricted under present law."[23] Congress had many concerns in a continued lack of oversight, but chief among them was the deterioration of the Fourth Amendment's vitality in the face of rapid technological changes.[24] Without such legislation, Congress recognized it would see the "gradual erosion of a precious right."[25] Thus, in enacting the ECPA, Congress struck what it believed to be "a fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement."[26] Title II of the

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

17. The Wiretap Act granted protection from eavesdropping to two types of nonelectronic communication: telephone conversations and face-to-face oral communication. 18 U.S.C. §§ 2510-2511 (1982).

18. *See* H.R. REP. NO. 99-647, at 17-19 (1986).

19. 425 U.S. at 440-41.

20. *See id.* at 440-41; *see* U.S. CONST. amend. IV. Congress later rectified this result through the passage of the Right to Financial Privacy Act of 1978. *See* 12 U.S.C. § 3402 (2012).

21. *See* H.R. REP. NO. 99-647, at 23; S. REP. NO. 99-541, at 3 (1986).

22. *See* The Electronic Communications Privacy Act, Pub. L. 99-508, 100 Stat. 1848 (1986).

23. H.R. REP. NO. 99-647, at 18.

24. *Id.*, at 19; S. REP. NO. 99-541, at 5. Congress listed many other concerns that may result from an absence of regulation, namely consumer skepticism of service providers, the threat of unauthorized third party acquisition of information, increased liability for law enforcement, and increased inadmissibility of evidence. H.R. REP. NO. 99-647, at 19; S. REP. NO. 99-541, at 5.

25. H.R. REP. NO. 99-647, at 19; S. REP. NO. 99-541, at 5.

26. H.R. REP. NO. 99-647, at 19; S. REP. NO. 99-541, at 5.

ECPA is known as SCA.[27] Section 2701 of the SCA prohibits "intentional . . . access . . . without authorization" of a "facility through which an electronic communication service is provided" in order to "obtain[], alter[], or prevent[] authorized access to a wire or electronic communication while it is in electronic storage."[28] Stored email content is considered "electronic storage" and is protected by the SCA.[29]

B. The Reach of the SCA's Investigative Tools

The SCA protects the user's privacy to contents stored by service providers in different ways depending upon a delineated distinction between two types of electronic services: electronic communication services (ECS) and remote computing services (RCS).[30] ECS is defined as "any service which provides to users thereof the ability to send or receive wire or electronic communications."[31] RCS is defined as "the provision to the public of computer storage or processing services by means of an electronic communications system."[32] The difference was greater in 1986 than it is today due to the proliferation of multifunctional service providers that provide joint ECS and RCS services.[33]

The SCA establishes conditions by which the government may compel a service provider to disclose the contents of a customer's account in § 2703.[34] Section 2703 requires that the government use one of two investigative tools to compel the service provider: an administrative subpoena or a search warrant.[35] Proper choice of investigative tool depends upon the nature of the content, the amount of

---

27. *In re* Warrant to Search a Certain E-Mail Account, 829 F.3d 197, 205 (2d Cir. 2016). *See* Stored Wire and Electronics Communications and Transactional Records Access, 18 U.S.C. §§ 2701-2712 (2012).

28. 18 U.S.C. § 2701(a) (2012).

29. *See* 18 U.S.C. § 2510(17)(A), (B) (2012) (defining "electronic storage" as "any temporary, intermediate storage of a wire or electronic communication incidental to the electronic transmission thereof" and "any storage of such communication by an electronic communication service for purposes of backup protection of such communication").

30. *See* 18 U.S.C. §§ 2702, 2703 (2012).

31. 18 U.S.C. § 2510(15)(2012).

32. 18 U.S.C. § 2711(2) (2012).

33. *See* Orin S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208, 1214 (2004) [hereinafter Kerr, *A User's Guide*] (noting the SCA's distinction "fr[oze] into the law the understandings of computer network use" as they were understood in 1986). Kerr rejects the "outdated" ECS-RCS distinction in favor of a single legal standard to all service providers. *See* Orin S. Kerr, *The Next Generation Communications Privacy Act*, 162 U. PA. L. REV. 373, 412 (2014) [hereinafter Kerr, *The Next Generation*].

34. 18 U.S.C. § 2703(c).

35. *See id.* Section 2703 also provides a third way, the 2703(d) order. *Id.* at (d).

time the content has been stored, and whether the service provider is an ECS provider or an RCS provider.[36]

The SCA's warrant provisions require that a warrant issued under the SCA must be issued in accordance with the Federal Rules of Criminal Procedure.[37] Rule 41 of the Federal Rules of Criminal Procedure, entitled "Search and Seizure," addresses the use of federal search warrants.[38] Rule 41(b)(5) governs the geographical reach of warrants authorized by a magistrate judge for property located "outside the jurisdiction of any state or district."[39] Issuance outside of such jurisdictions is limited to "a United States territory, possession or commonwealth;" "the premises . . . of a United States diplomatic or consular mission in a foreign state;" or "a residence and any appurtenant land owned or leased by the United States and used by United States personnel assigned to a United States diplomatic or consular mission in a foreign state."[40] When the government compels a third party service provider to disclose customer records via warrant, that third party becomes an agent of the government.[41] That third party is accordingly restricted by the full force of the Fourth Amendment in its execution of the warrant.[42]

The SCA's subpoena provisions may enable a much broader reach for the government. In *Marc Rich & Co., A.G. v. United States*, the United States Court of Appeals for the Second Circuit allowed the use of a grand jury subpoena to compel overseas production of a Swiss commodities trading group's business records in a tax evasion investigation.[43]

---

36. *See id.* at (a)-(c). A warrant may be used in order to obtain email contents in ECS storage for less than 180 days and email contents in RCS storage. *Id.* at (a), (b). A subpoena may be used without provided notice to the user in order to obtain basic information, such as a user's name or address. *Id.* at (c)(2). A subpoena may be used once notice has been provided to the user in order to obtain email contents in ECS storage for longer than 180 days and email contents in RCS storage (as an alternative to a warrant). *Id.* at (a), (b)(1)(B).

Kerr explains the traditional interpretation of the distinction would categorize unopened email in a user's inbox as content stored by an ECS provider and opened email stored on the user's account as content stored by an RCS provider. *See* Kerr, *A User's Guide*, *supra* note 33, at 1216. However, the Ninth Circuit interprets all email stored as content stored by an ECS provider, regardless of whether it has been opened, until the "underlying message has expired in the normal course." *See* Theofel v. Farey-Jones, 359 F.3d 1066, 1070 (9th Cir. 2004). The term "normal course" has not yet been defined by the Ninth Circuit. Kerr, *A User's Guide*, *supra* note 33, at 1218.

37. *See* 18 U.S.C. § 2703(a), (b)(1)(A).

38. FED. R. CRIM. P. 41.

39. *Id.* at 41(b)(5).

40. *Id.*

41. *See* Coolidge v. New Hampshire, 403 U.S. 443, 487 (1971).

42. *See id.*

43. Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 666-67 (2d Cir. 1983).

Unlike a warrant, which is restricted by Rule 41's geographical limitations based on the location of the seized property,[44] the Second Circuit reasoned that a grand jury subpoena is restricted by whom controls the documents, not where the documents are located.[45] Although the issue has never been squarely decided, the SCA's subpoena provisions may accordingly possess such broad reach as to lawfully compel a third party service provider to produce a user's content stored in a foreign sovereign.[46]

C. The Morrison *Framework*

In *Morrison v. National Australian Bank Ltd.*, the United States Supreme Court developed a framework to analyze a statute's potential extraterritorial effect in light of the presumption against extraterritoriality.[47] The presumption against extraterritoriality is a "longstanding principle of American law 'that legislation of Congress, unless a contrary intent appears, is meant *to apply* only within the territorial jurisdiction of the United States.'"[48] Initially, the court must determine if the presumption has been rebutted.[49] The presumption can only be rebutted if there is "'affirmative intention of the Congress clearly expressed' to give a statute extraterritorial effect."[50] Thus, a statute will only rebut the presumption against extraterritoriality if it clearly provides affirmative indication to the contrary.[51]

If the court finds no affirmative indication of extraterritoriality, the court must determine whether the presented case implicates an extraterritorial application or a domestic application of the statute.[52] Nearly all extraterritorial cases have some mix of foreign and domestic action;[53] consequently, the court must determine which conduct the

---

44. FED. R. CRIM. P. 41.

45. *Marc Rich*, 707 F.2d at 667. The Second Circuit further expounded upon the grand jury subpoena's pervasive reach, stating a served individual may not "resist the production of documents on the ground that the documents are located abroad." *Id.*

46. *See id.*

47. *See* Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247 (2010).

48. EEOC v. Arabian Am. Oil Co., 499 U.S. 244, 248, (1991) (quoting Foley Bros., Inc. v. Filardo, 336 U.S. 281, 285 (1949)).

49. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101 (2016); *Morrison*, 561 U.S. at 255.

50. *Morrison*, 561 U.S. at 255 (quoting *Arabian Am.*, 499 U.S. at 248).

51. *See id.* at 265.

52. *See id.* at 266; *see also RJR Nabisco*, 136 S. Ct. at 2101.

53. "For it is a rare case of prohibited extraterritorial application that lacks *all* contact with the territory of the United States. But the presumption against extraterritorial application would be a craven watchdog indeed if it retreated to its kennel whenever *some* domestic activity is involved in the case." *Morrison*, 561 U.S. at 266.

statute was primarily intended to prevent.[54] It must first identify the statute's "focus" or "objects of . . . solicitude" and then look at the facts through that prism in order to determine if the challenged application truly involves extraterritorial application.[55] If the conduct relevant to the statute's focus took place within United States territory, the statute's application is lawful, despite some conduct occurring extraterritorially.[56] If the conduct relevant to the statute's focus took place outside of United States territory, the statute's application is unlawful, despite some conduct occurring domestically.[57]

III. COURT'S DECISION

In the noted case, the Second Circuit applied the *Morrison* framework to analyze whether the SCA's warrant provisions had an extraterritorial effect.[58] First, the court examined the text of § 2703's warrant provisions to determine if the provisions gave "affirmative indication" of extraterritorial effect.[59] Second, the court analyzed the nature of an SCA "warrant," considering whether it was a traditional warrant or a hybrid warrant-subpoena.[60]

The court then analyzed whether enforcement of an SCA warrant to compel a third party service provider to disclose email contents stored on a server in Ireland would constitute extraterritorial application or domestic application.[61] Accordingly, third, having determined the SCA's warrant provisions had no extraterritorial effect, the court identified the "focus" of the SCA warrant provisions by studying the language of warrant provisions, the language of other parts of the SCA, and the legislative history of the act.[62] Fourth, the court analyzed whether enforcement of an SCA warrant served to an email service provider to disclose email contents stored on servers located in a foreign sovereign is an extraterritorial application or a domestic application of the warrant provisions.[63] Ultimately, the court held that enforcement of an SCA

---

54. *See id.*
55. *See id.* at 266-70.
56. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2101 (2016).
57. *Id.*
58. *In re* Warrant to Search a Certain E-Mail Account, 829 F.3d 197, 210 (2nd Cir. 2016).
59. *See id.* at 211.
60. *See id.* at 214-16.
61. *See id.* at 220.
62. *Id.* at 217-20.
63. *Id.* at 220-21.

warrant against a United States company for production of contents stored on servers located outside the United States is beyond the enforceable bounds of the law's warrant provisions, and the enforcement of such a warrant would constitute an unlawful extraterritorial application.[64]

A. The SCA's Warrant Provisions Lack Extraterritorial Enforceability

First, the Second Circuit briefly examined the text of the warrant provisions to determine if they provided extraterritorial application.[65] It acknowledged past Supreme Court jurisprudence of a presumption against extraterritoriality elucidated in *Morrison*, where Congressional legislation is presumed to apply only within the jurisdictional bounds of the United States unless the legislation clearly indicates otherwise.[66] Examining § 2703 of the SCA, the court found no indication of any intention of extraterritorial application.[67] The court found it "particularly unlikely" for the act to intend extraterritorial effect without "affirmative indication."[68] Consequently, the court held the SCA's warrant provisions had no extraterritorial effect.[69]

Second, the court analyzed the nature of the SCA "warrant," weighing Microsoft's argument for a traditional warrant against the government's argument for a hybrid warrant-subpoena, which was adopted by the lower court.[70] The court noted the assumption that Congress uses legal terms of art in legislation fully aware of the term's legal meaning and its implications.[71] It also considered the balance between the Constitution's Fourth Amendment restrictions upon warrants and the invasive power of law enforcement's need to use warrants in order to seize evidence.[72] The court then noted the restrictions of the SCA's warrant provisions, namely the need for all SCA warrants to adhere to the Federal Rules of Criminal Procedure.[73] It found this restriction provided evidence of legislative intent to treat the SCA warrant as a traditional warrant.[74] The court distinguished the reach of a

64. *Id.* at 222.
65. *Id.* at 211.
66. *Id.* (citing Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010)).
67. *Id.* at 211.
68. *Id.*
69. *See id.*
70. *See id.* at 214-16.
71. *Id.* at 212 (citing Fed. Aviation Admin. v. Cooper, 132 S. Ct. 1441, 1449 (2012)).
72. *See id.*
73. *Id.* at 207-08, 211; *see also* FED. R. CRIM. P. 41.
74. *In re Warrant*, 829 F.3d at 213.

traditional warrant, which is confined to domestic application, from the reach of a subpoena, which may have extraterritorial application.[75] The court examined § 2703 of the SCA, entitled "Required disclosure of customer communications or records,"[76] and found a distinction between circumstances that constitute proper use of a warrant and circumstances that constitute proper use of a subpoena.[77] Specifically, the court found the SCA "recognizes this distinction and, unsurprisingly, uses the 'warrant' requirement to signal (and to provide) a greater level of protection to priority stored communications, and 'subpoenas' to signal (and provide) a lesser level."[78] As such, the Second Circuit rejected the government's argument that an SCA warrant is executed as a subpoena, should be treated as a hybrid warrant-subpoena, and should be subject to the extensive reach provided in *Marc Rich*.[79] Consequently, the Second Circuit held that an SCA warrant was restrained to the traditional limits of a warrant—domestic application only.[80] Thus, the SCA warrant provisions did not rebut the presumption against extraterritoriality.[81]

B. Unlawful Extraterritorial Application of an SCA Warrant to Servers Overseas

Third, having determined the presumption against extraterritoriality applied to the SCA's warrant provisions, the court began to analyze whether the enforcement of the warrant would qualify as unlawful extraterritorial application by identifying the underlying focus of the SCA's warrant provisions.[82] The court explained, "[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."[83] The court first looked to the SCA's warrant provisions themselves.[84] It acknowledged the understanding of the term "warrant" had historically carried restrictions meant to maintain individual privacy protections.[85]

---

75. *See id.* at 214-16.
76. 18 U.S.C. § 2703 (2012).
77. *See In re Warrant*, 829 F.3d at 214.
78. *Id.* (citing 18 U.S.C. § 2703(a), (b)(1)(A) (2012)).
79. *Id.* at 215.
80. *See id.* at 216.
81. *See id.*
82. *Id.*
83. *Id.* (quoting *Morrison*, 561 U.S. at 267).
84. *See id.* at 217.
85. *Id.*

Further, the court reasoned, the SCA's schema for determining the appropriate investigative tool also determines the user's appropriate level of privacy expectation.[86] Therefore, the user's expectation of privacy determines the appropriate investigate tool's reach according to its statutory procedural restrictions.[87] Accordingly, if the circumstances of the storage evoked such a historically loaded term, the privacy protections that come with that term are also evoked.[88] Thus, the court ruled the warrant provisions' "focus" is privacy.[89] The court then looked at the two preceding sections of the SCA[90] and found their intended protection went beyond mere disclosure of information by third parties; it "shelter[ed] the communications' integrity."[91] Thus, the court determined the "focus" of the SCA as a whole was the protection of the user's privacy.[92] Finally, the court looked to the legislative history of the SCA both upon enactment[93] and throughout amending legislation[94] and again determined the SCA's primary purpose is the protection of privacy interests.[95] The court determined these sources provided adequate evidence of a "focus" to protect individual privacy interests.[96] In doing so, the court rejected the government's argument that the SCA's primary purpose was to protect disclosure rather than privacy.[97] Thus, the court ultimately determined the "focus" of the SCA, the "'object[] of the statute's solicitude,'" was the protection of the user's privacy rights.[98]

Fourth, the court contemplated where the conduct relevant to the warrant provisions' "focus" took place in order to determine if enforcement would constitute unlawful extraterritorial application.[99] The

---

86 *Id.*
87. *Id.*
88. *See id.*
89. *Id.*
90. *See* 18 U.S.C. §§ 2701, 2702 (2012).
91. *In re Warrant*, 829 F.3d at 218.
92. *Id.* at 219.
93. *Id.* (examining S. REP. NO. 99-541, at 3 (1986) (indicating the advances in technology threatened Americans' privacy interests); H.R. REP. NO. 99-647, at 23 (1986) (focusing concern of Internet service customers' limited ability to prevent disclosure of their private records maintained by Internet service providers)).
94. *See id.* at 213 (noting no substantial changes were made regarding the SCA warrant's reach in the Uniting and Strengthening America by Providing Appropriate Tools Required To Intercept and Obstruct Terrorism Act (USA Patriot Act) Act of 2001, Pub. L. 107–56, § 220, 115 Stat. 272, 291-92 (2001)).
95. *In re Warrant*, 829 F.3d at 219.
96. *Id.* at 220.
97. *Id.* at 218; *see also* 18 U.S.C. § 2703(a) (2012).
98. *In re Warrant*, 829 F.3d at 216.
99. *See id.* at 220-21.

court found the invasion of the user's privacy occurred where the content was stored—Dublin, Ireland.[100] The court rejected the lower court's reasoning that no extraterritorial action was necessary because Microsoft did not need to physically step onto foreign soil in order to produce the content to the government.[101] The court countered by asserting that Microsoft's necessary interaction with its Dublin-based datacenter to initially collect the content would constitute extraterritorial action.[102] The court also rejected the government's argument that the relevant conduct was the disclosure of the content, which would take place domestically.[103] The court found this argument was predicated upon a finding of disclosure as the "focus" of the warrant provision and was therefore irrelevant.[104] Hence, the court found that production of content stored on servers overseas would be an extraterritorial application of the SCA warrant.[105] Therefore, the Second Circuit concluded that an SCA warrant for content stored on servers located on a foreign sovereign had no enforceability because the SCA's warrant provisions do not extend to extraterritorial application and any such application would be unlawful.[106]

In his concurrence, Judge Gerard E. Lynch rejected the majority's framing of the issue as a government threat to individual privacy; rather, he determined the real issue at hand was the international reach, or lack thereof, of an SCA warrant.[107] He agreed that the SCA itself did not give grant extraterritorial application,[108] but he was not fully persuaded of a singular "focus" to protect individual privacy in electronic communication.[109] Nor was he persuaded that an SCA "warrant" was truly a warrant in the traditional legal sense of the term.[110] Further, Judge Lynch was wary of the practical consequences this ruling would permit, most notably the ability for an individual to obtain "absolute" protection of his email contents by merely misrepresenting his location.[111] Judge Lynch stressed the need for Congress to revisit the statute and contemplate reforms that would "weigh[] the costs and benefits of authorizing court

100. *Id.* at 220.
101. *Id.*
102. *Id.*
103. *Id.* at 218.
104. *See id.* at 220.
105. *Id.*
106. *Id.* at 222.
107. *See id.* at 225 (Lynch, J., concurring).
108. *Id.* at 226.
109. *See id.* at 229.
110. *Id.* at 226.
111. *See id.* at 224, 230.

orders of the sort at issue in this case."[112] Ultimately though, he acknowledged the question is not whether Congress would have intended the statute to have extraterritorial effect, but whether Congress expressed that clear intent of extraterritorial effect.[113] Thus, finding no clear intent, Judge Lynch concurred with the majority's result while rebuffing it as a victory for privacy rights in a much narrower opinion.[114]

IV. ANALYSIS

In an important case for privacy rights, the Second Circuit correctly decided an SCA warrant bears no lawful extraterritorial enforceability to email contents stored on servers in foreign countries. SCA warrants should be treated according to the restrictions of traditional warrants.[115] The rigidity of these restrictions should be controlled by an appropriate level of privacy interest, determinable by the circumstances by which those contents have been acquired by the service provider. The SCA aptly addresses these circumstances and requires adherence to suitably stringent demands. However, the inadequate pace of legislation[116] has opened the door to many potential concerns when privacy protections of the SCA are applied.[117]

The "fair balance between the privacy expectations of citizens and the legitimate needs of law enforcement"[118] originally weighed by Congress before enacting the ECPA appears to have shifted much of the burden to law enforcement due to the ramifications of this decision.[119] Without the ability to utilize the SCA warrant provisions to obtain content stored on servers overseas, the efficiency of law enforcement is now dependent upon the interests of a foreign sovereign.[120] These

---

112. *Id.* at 231.

113. *Id.* at 226.

114. *See id.* at 233.

115. *See* Fed. Aviation Admin. v. Cooper, 132 S. Ct. 1441, 1449 (2012) (asserting when Congress uses a legal term of art, it understands the term's meaning and implications).

116. *See* Kerr, *A User's Guide*, *supra* note 33; Kerr, *The Next Generation*, *supra* note 33.

117. *See In re Warrant*, 829 F.3d at 221 (Carney, J., majority); *id.* at 230 (Lynch, J., concurring).

118. H.R. REP. NO. 99-647, at 19 (1986); S. REP. NO. 99-541, at 5 (1986).

119. *See In re Warrant*, 829 F.3d at 221 (Carney, J., majority) (acknowledging this decision places a "substantial burden on the government" and may "seriously impede law enforcement efforts").

120. *See id.* The current process for obtaining content stored on servers overseas is governed by Mutual Legal Assistance Treaties (MLATs) signed by the United States and other countries. *Id.* For MLAT-participating countries, the government must request the country's assistance in executing the warrant. U.S. DEP'T OF STATE, 7 FOREIGN AFFAIRS MANUAL § 962.1

sovereigns could in turn skirt their natural obligations to aid in crime prevention, leaving United States law enforcement little recourse.[121] Nevertheless, the imposition of American law on foreign sovereigns also comes at a diplomatic cost that must be considered before a court decides to expand a statute's territoriality.[122] The presumption against extraterritoriality should not be defeated by a heavy burden upon law enforcement.

The pace of technology has made the SCA's governmental restrictions susceptible to exploitation for the purpose of evading law enforcement efforts in light of the majority's decision. It is not hard to imagine a service provider, perhaps a new entrant into the industry, marketing its overseas servers as an attractive feature with the implicit understanding that a criminal user's content will be out of reach of federal SCA warrants. One can imagine an informed wrongdoer capitalizing on the court's decision by misrepresenting his geographical location to a service provider who relies solely on the user's locational representation to decide where to store the user's contents.[123] Law enforcement has no easily obtainable weapons to combat this threat under current statute. Nevertheless, it is the legislature's job, not the court's, to address such concerns.

Admirably, the court was not persuaded to endanger individual privacy rights in order to alleviate the "substantial burden" placed upon law enforcement by the aforementioned concerns.[124] The majority's decision took a well-placed step in the right direction and set a strong precedent for protection against the "gradual erosion"[125] of privacy created by encroaching governmental action. If often discussed SCA reform proposals[126] begin to include extraterritorial application, such laws should be stringently scrutinized to determine if they infringe upon the "precious right"[127] of individual privacy.

Joseph Schrempp*

(2013). For non-MLAT-participating countries, there is no formal tool law enforcement may use to facilitate a search warrant's execution. *In re Warrant*, 829 F.3d at 221.

121. *See id.* at 221.

122. *See id.*

123. *See id.* at 230 (Lynch, J., concurring).

124. *See id.* at 221 (Carney, J., majority).

125. H.R. REP. NO. 99-647, at 19 (1986); S. REP. NO. 99-541, at 5 (1986).

126. *See* Kerr, *The Next Generation*, supra note 33, at 386-90.

127. H.R. REP. NO. 99-647, at 19; S. REP. NO. 99-541, at 5.

* © 2016 Joseph Schrempp. Junior Member, Volume 19, *Tulane Journal of Technology and Intellectual Property.* J.D. candidate 2018, Tulane Law School; B.B.A. 2014, Finance and Risk Management/Insurance, University of Georgia. The author would like to thank his family and friends for their support and *JTIP*'s members for their hard work and dedication to the *Journal.*