Journal of Technology Law & Policy

Volume 22 | Issue 2 Article 5

January 2018

Extraterritorial Application of Data Privacy Law: How the Stored Communication Act Lags Behind Modern Technology

Andrew Bayudan

CASE COMMENT

EXTRATERRITORIAL APPLICATION OF DATA PRIVACY LAW: HOW THE STORED COMMUNICATION ACT LAGS BEHIND MODERN TECHNOLOGY

Andrew Bayudan[*]

I. OVERVIEW

The Stored Communications Act (SCA),[1] which allows the government to compel the production of electronic customer information from Internet Service Providers (ISPs), was found to be limited in scope by the Second Circuit in *Microsoft Corp. v. United States*.[2] The Second Circuit ruled that the SCA did not permit the government to force ISPs to hand over data that is located outside the United States.[3]

In 2013, a warrant served under the SCA, was authorized requiring Microsoft to produce information and emails related to a federal criminal investigation.[4] Many of the emails demanded by the warrant were located on a data server in Ireland.[5] Since these emails were outside the United States, Microsoft argued that the warrant under the SCA had no jurisdiction in Ireland and moved for the warrant to be quashed.[6] The magistrate judge denied the motion.[7] The denial was also affirmed by the Southern District of New York, reasoning that the SCA compelled those served with warrants under the SCA to produce information regardless of the information's location.[8] Microsoft appealed the district court's decision,[9] held that the district court's denial of microsoft's motion to quash the warrant was improper and the case should be reversed and remanded to the district court.[10]

---

* Andrew Bayudan, J.D. Candidate, May 2019, University of Florida Levin College of Law. I would like to thank my family for their love and support.

1. 18 U.S.C. § 2703 (2009).
2. Microsoft v. United States, 829 F.3d 197, 201–02 (2d Cir. 2016).
3. *Id.*
4. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 467 (S.D.N.Y. 2014).
5. *Microsoft*, 829 F.3d at 200.
6. *Id.* at 200–01.
7. *Id.* at 201.
8. *Warrant to Search*, 15 F. Supp. 3d at 477.
9. *Microsoft*, 829 F.3d at 200.
10. *Id.* at 201.

II. BACKGROUND

A. *Microsoft's Email Services*

Microsoft is an ISP headquartered and incorporated in the United States.[11] Microsoft provides free online email services to the public.[12] When creating an email account, users are asked to indicate their location of residence.[13] The information associated with a user's account, along with the emails sent and received through the account, is stored on physical servers that are housed in large datacenters.[14] The datacenters are generally located near the location the user initially indicated when creating the email account.[15] This email service is offered to customers in over 100 countries and Microsoft maintains datacenters in over forty countries.[16]

Though Microsoft's datacenters are located worldwide, the company is able to manage and collect information on servers in other countries through its database management computer program from the United States.[17] This computer program can be accessed in offices in the United States. Additionally, this computer program allows Microsoft to retrieve data located on servers in other countries and store it on servers in the United States.[18] Therefore, Microsoft employees in the United States do not need to travel outside the United States to collect information from servers located in other countries.[19]

B. *The Stored Communications Act*

The U.S. Government served a warrant on Microsoft to produce certain electronic information under the authority of the SCA.[20] In 1986, the SCA was passed to protect American privacy interests in response to the rapidly evolving and advancing technologies that developed alongside the personal computer.[21] The SCA prohibits unauthorized parties to access or modify electronic communications maintained by ISPs.[22] Yet, the SCA also contains a provision that requires ISPs to

---

11. *Id.* at 202.
12. *Id.*
13. *Id.*
14. *Id.*
15. *Id.*
16. *Id.*
17. *See id.* at 203.
18. *Id.*
19. *Id.*
20. *Id.* at 205.
21. *Id.*
22. *Id.* at 207; *see* 18 U.S.C. § 2702 (2012).

provide data that the government so requests with a warrant, pursuant to the Federal Rules of Criminal Procedure.[23] The SCA did not, however, contain any provisions that address whether the issued warrants would be applied to electronic communications outside the United States.[24]

C. *The SCA's Extraterritorial Scope*

A two-part test adopted from *Morrison v. Nat'l Austl. Bank Ltd.* to determine whether the SCA can apply to extraterritorial electronic communications is used to interpret the SCA.[25] The first part of the test looks at whether the statute's language suggests extraterritorial applications.[26] When interpreting a statute, there is a default presumption that Congress enacted the statute with the intent to apply the statute only within the United States.[27] This part of the test requires that the statutory language has a clear indication that the statute would apply extraterritorially.[28]

For the second part of the test, it has to be determined whether the application of the statute in the disputed case is an unlawful and extraterritorial application.[29] In this part of the test, the facts surrounding the case and the statute's focus are examined.[30]

D. *The District Court's Reasoning*

The district court, finding that the SCA warrant could be enforced extraterritorially, focused on the ambiguity of the SCA's use of the word "warrant".[31] The district court stated that a warrant, in the context of the SCA, actually is a hybrid of a warrant and a subpoena.[32] The SCA warrant is like a traditional search warrant because the SCA warrant must be obtained by following the Federal Rules of Criminal Procedure.[33] The SCA warrant is like a subpoena because the receiver of the SCA warrant

---

23. 18 U.S.C. § 2703(a) (2012).

24. *Microsoft*, 829 F.3d at 208.

25. *See generally* Morrison v. Nat'l Austl. Bank, Ltd., 561 U.S. 247 (2010); *Microsoft*, 829 F.3d at 209.

26. *Microsoft*, 829 F.3d at 210.

27. *Id.*

28. *Id.*; *see also Morrison*, 561 U.S. at 247.

29. *Microsoft*, 829 F.3d at 210.

30. *Id.*

31. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 467, 470 (S.D.N.Y. 2014).

32. *Id.* at 471.

33. *Id.* at 470.

must provide the requested information no matter the information's location.[34]

The district court also considered the practical effects of not compelling Microsoft to produce the email data from extraterritorial servers.[35] By not compelling Microsoft to do so, criminals could simply avoid SCA warrants by moving their servers to other counties.[36] This would also result in the government having to turn to Mutual Legal Assistance Treaties (MLATs) to obtain information stored extraterritorially.[37] MLATs are international agreements where one country can request assistance from another country with criminal investigations that have effects in other countries.[38] Since MLATs rely on the cooperation of another country's government, MLATs often operate very slowly.[39] Additionally, the United States does not have MLATs with many countries, making it easier for criminals to avoid SCA warrants.[40]

III. THE INSTANT CASE

In the instant case, the Second Circuit applied the two-part *Morrison* Test to determine whether or not the warrant under the SCA could be applied to the email located on servers in Ireland.[41] Reversing the district court's decision, the Second Circuit decided that the SCA warrant could not compel Microsoft to produce data located on Ireland's servers.[42]

For the first part of the *Morrison* test, the court found that Congress did not expressly indicate their intent for the SCA to apply extraterritorially.[43] There is no textual or documentary support to suggest that the SCA applies extraterritorially and reading the SCA to have an extraterritorial scope is arbitrarily expanding the SCA's reach.[44]

The court further explained that the district court's interpretation of the word "warrant" was incorrect.[45] The court found that the district court inappropriately interpreted "warrant" as having a hybrid meaning.[46]

---

34. *Id.* at 471–72.
35. *Id.* at 474–75.
36. *Id.*
37. *Id.* at 476.
38. *Id.*
39. *Id.*
40. *Id.*
41. Microsoft Corp. v. United States, 829 F.3d 179, 210 (2d Cir. 2016).
42. *Id.*
43. *Id.* at 211.
44. *Id.*
45. *Id.* at 212.
46. *Id.* at 210.

Instead, the court held that "warrant" under the SCA had a meaning only related to the privacy protections granted by the Fourth Amendment.[47]

Turning to the second part of the *Morrison* test, the court determined that using an SCA warrant to compel Microsoft to produce electronic information located on a server in Ireland was an extraterritorial application of the SCA.[48] The SCA was primarily enacted to protect and focus on citizens' privacy, as evidenced by the SCA being part of the larger Electronic Communications Privacy Act.[49] Further, the SCA's warrant to Microsoft was being used to assist a criminal investigation, rather than protecting a citizen's privacy interest.[50] The SCA warrant issued to Microsoft targeted information on data servers located in Ireland.[51] Because the focus of the SCA warrant was a privacy interest that existed in Ireland, this application of the SCA was extraterritorial and outside the SCA's scope.[52]

IV. ANALYSIS

This case was decided incorrectly because the court failed to consider the technological advancements that have occurred since the initial creation of the SCA. The SCA was passed in 1986, where the state of technology was vastly different and inferior to the state of technology today. Since 1986, both the amount of storable data and the easiness of storing data have greatly increased, while the cost of storing data has decreased. Additionally, developments in the internet have made it very easy to transport and store data across large distances at extremely fast speeds. When the SCA was initially passed, these advancements were likely never considered or realized. Many of the technological obstacles that existed in the 1980s that posed practical problems in extraterritorially enforcing the SCA warrant no longer exist today.

Microsoft, like many other large corporations that maintain large amounts of electronic data and have numerous customers around the world, has data located in many other countries. Microsoft can easily move data on one country's server to another without much burden or cost to the company. To limit the enforcement of an SCA warrant to only data located on servers within the United States would obstruct government and criminal investigations. This limitation makes little sense in a world where large amounts of data is constantly moving across

47. *Id.*
48. *Id.* at 213.
49. *Id.* at 217.
50. *Id.*
51. *Id.* at 216.
52. *Id.* at 220.

borders at high speeds with little cost. The court, rather than looking at where the data servers are located, should have given more weight to where the ISP was located and the extent of the ISPs business in the involved countries when determining if the SCA warrant could be enforced.

This case also exemplifies how the SCA's language and goals have been outdated and outpaced by technology. The SCA lacks many of the considerations and concerns that have developed since its enactment. The court, rather than choosing to acknowledge these advancements, chose to adopt a limited and archaic view of the SCA that prevents the court from fully addressing the issues in this case.

V. CONCLUSION

The decision in *Microsoft Corp. v. United States* challenged the scope of the SCA. The Second Circuit, not taking into account the numerous technological advancements since the SCA was passed, incorrectly limited the enforcement of SCA warrants to only data that exists domestically. This decision could have many undesirable consequences, including criminals avoiding government SCA warrants. These issues will continue to exist and pose problems for courts as technology rapidly evolves.