Vanderbilt Journal of Transnational Law

Volume 49
Issue 5 *November 2016*

Article 5

2016

Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers

Matthew McKenna

NOTES

Up in the Cloud: Finding Common Ground in Providing for Law Enforcement Access to Data Held by Cloud Computing Service Providers

ABSTRACT

Cloud computing is an everyday part of the modern world; a technology that is increasingly transcending international borders. Disregarding international borders allows cloud computing to operate more efficiently and thus provides better service to users. Yet, the global nature of cloud computing raises a question—what happens if multiple countries apply facially similar laws to cloud computing providers differently? This scenario is common, especially in the context of law enforcement seeking access to cloud computing data. The United States and the United Kingdom have similar laws regarding the government's ability to acquire users' data. Importantly, neither law explicitly addresses the question of if and how the law can be applied in a setting where traditional physical borders are being ignored. Currently, both laws focus on the location of the cloud service provider. Instead, these laws should focus on the user's nationality, or the location from where the data was created. This approach would alleviate some of the problems existing today, including the trend toward data localization through increased regulation of cloud computing. However, this solution will not be successful unless the Mutual Legal Assistance Treaty process is reformed as well.

TABLE OF CONTENTS

I. INTRODUCTION

Cloud computing is a ubiquitous feature in today's increasingly connected world. A consumer uses cloud computing when accessing emails through Google mail, streaming songs on Spotify or iTunes, or working on papers in Google Docs.[1] Individual consumers are not the only ones using cloud computing services. According to a 2012 survey, eight in ten companies use cloud computing services as part of their information technology (IT) operations as a way to increase efficiency and decrease operating costs.[2] Simply put, anytime someone accesses data stored on the Internet and not on a computer hard drive, that data is being accessed using the "cloud."[3]

Despite its ubiquity, the rise of cloud computing has not been without controversy. For example, cloud computing implicates the tension between individuals' data privacy rights and national security concerns. [4] Apart from domestic citizens' concerns over law

---

1. *See* Mark Koba, *Cloud Computing 101: Learning the Basics*, CNBC (June 2, 2011, 11:03 AM), http://www.cnbc.com/id/43077233 [https://perma.cc/THQ9-6PQA] (archived Oct. 11, 2016) (describing the ways consumers normally access the cloud including email, social networks, and online software); *see also* Michael Miller, *Comparing Google Docs with Competing Cloud Computing Applications*, QUE (Feb. 9, 2009), http://www.quepublishing.com/articles/article.aspx?p=1323244 [https://perma.cc/E692-77D6] (archived Oct. 11, 2016) (discussing several cloud computing applications for writing including Google Docs).

2. *See* Ned Smith, *Why More Businesses Are Using Cloud Computing*, CNBC (July 25, 2012, 1:00 PM), http://www.cnbc.com/id/48319526 [https://perma.cc/BA9S-VDCZ] (archived Oct. 11, 2016) (summarizing the findings of a survey sponsored by an IT industry trade association).

3. *See* Koba, *supra* note 1 (noting that "the cloud" is merely "a metaphor for the Internet").

4. For an overview of the many issues currently surrounding technology, privacy, and law enforcement in an international context see *Safety, Privacy, and the Internet Paradox: Solutions at Hand and the Need for New Trans-Atlantic Rules*, MICROSOFT CORPORATE BLOGS (Jan. 20, 2015), http://blogs.microsoft.com/on-the-

enforcement access, cloud computing also raises questions over the extraterritorial reach of countries' laws and its effect on international jurisdiction.[5]

The tension between cloud computing and its implications on international jurisdiction remained a largely academic issue until recently. In 2014, the Southern District of New York decided *In re Matter of a Warrant to Search a Certain E-mail Account Controlled and Maintained by Microsoft Corporation*[6] ["The Microsoft case"], a case which highlights the international legal consequences of cloud computing. At issue was whether the United States could compel Microsoft to hand over a foreign person's email data stored on a Microsoft server in a foreign country merely because Microsoft is headquartered in the United States.[7] A magistrate judge ruled that the United States has the power to compel Microsoft to hand over the data, irrespective of any extraterritorial concerns, because of the powers given to law enforcement under the Stored Communications Act (SCA).[8] The magistrate judge's decision was upheld on appeal by the district court.[9] However, in 2016, the Second Circuit overturned the warrant compelling Microsoft to hand over the data stored overseas.[10] The court found that Congress did not intend the SCA, the main law covering law enforcement access to computer data, to apply extraterritorially.[11]

This Note does not analyze the outcome of the case or the Second Circuit's reasoning. Rather, the discussion of the case illustrates the issues that must be resolved by the United States and other countries when deciding how to handle the acquisition of data stored in the cloud. The questions raised by the Microsoft case will arise more frequently as law enforcement agencies around the world rely on increasingly outdated statutes to gain access to information stored on the cloud. Currently, the international community's focus is on the United States'

---

issues/2015/01/20/brad-smith-time-nations-adapt-laws-reflect-todays-technology/ [https://perma.cc/RJ9H-YR7A] (archived Oct. 11, 2016).

5. *See generally* Vineeth Narayanan, *Harnessing the Cloud: International Law Implications of Cloud-Computing*, 12 CHI. J. INT'L L. 783 (2012).

6. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) [hereinafter *Microsoft Case*].

7. *Id.* at 467.

8. *Id.* at 470.

9. Ellen Nakashima, *Judge Orders Microsoft to Turn Over Data Held Overseas*, WASH. POST (July 31, 2014), https://www.washingtonpost.com/world/national-security/judge-orders-microsoft-to-turn-over-data-held-overseas/2014/07/31/b07c4952-18d4-11e4-9e3b-7f2f110c6265_story.html [https://perma.cc/GT38-6R8F] (archived Oct. 11, 2016) (reporting on the "surprise" bench ruling by the district court judge in upholding the magistrate judge's decision).

10. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016).

11. *Id.* at 201.

allegedly broad powers to access data anywhere in the world.[12] As will be discussed, the United States is not the only country with ambiguous laws that grant law enforcement broad powers. Consequently, if these issues are left unresolved, other countries could start seeing more cases like the Microsoft case.

This Note examines several issues related to law enforcement access to cloud computing. First, a comparison with the United Kingdom's statute on law enforcement access shows that the SCA is not unique in the powers it gives to law enforcement, at least textually. Next, this Note examines whether relying on the traditional principles of international jurisdiction can help ameliorate the current issues surrounding law enforcement access to something that is inherently international in scope.

A discussion on the way countries approach this issue not only affects diplomatic relations but also affects the future of the entire cloud computing industry, which is comprised mainly of U.S. companies.[13] Part II discusses the basics of cloud computing to show why it naturally implicates international concerns. Part II also briefly describes the Microsoft case before concluding with a summary on the general principles of international jurisdiction. Part III compares analogous U.S. and UK statutes covering law enforcement access to the cloud to illustrate why it is wrong for foreign leaders and other commentators to single out the United States for its allegedly broad surveillance powers. Despite the favorable ruling for Microsoft, the Second Circuit's decision does not fix the greater international issues raised by cloud computing. While this juxtaposition is restricted to only two countries, it shows that a new approach or solution is needed. Part IV discusses possible solutions to the problem of law enforcement access to the cloud. In the end, this Note provides a solution that is not only possible to achieve, but also leads to greater certainty for businesses and respect for international norms.

II. SETTING THE STAKES FOR WHY CLOUD COMPUTING IS DIFFERENT

A. *What Is Cloud Computing?*

To understand how cloud computing has given rise to the controversy of law enforcement access to data in the cloud, one should understand what cloud computing is and how it works. According to

---

12. Nakashima, *supra* note 9 (noting that the district court's decision will most likely lead to more outrage from foreign officials).

13. *See* 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/#330e5ca48c8b [https://perma.cc/MDR9-UUFM] (archived Oct. 11, 2016) (discussing Germany's efforts in protecting data from NSA's reach).

the National Institute of Standards and Technology, the technical definition of "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources . . . that can be rapidly provisioned and released with minimal management effort."[14] To put it another way, cloud computing's focus is with the on-demand delivery of computing power, software, storage services, and other platforms to customers over the Internet.[15]

As mentioned, most people are probably familiar with cloud computing because they interact with it every day when accessing emails on Gmail, Microsoft Outlook, or Yahoo!. These programs, also known as "email clients," house data on servers that are separate from your computer.[16] Provided one has Internet access, one can access emails stored on an email client anywhere in the world. Email clients, which in general work on the same principles as cloud computing, are just one example of what cloud computing is. Essentially, cloud computing gives consumers and businesses the ability to use programs and save data over the Internet rather than on a personal hard drive located on the user's computer. This can result in cost savings on IT operations for businesses and provide users the benefit of data mobility.[17]

Currently, there are three types of cloud computing services offered by companies: Software as a Service (SaaS), Platform as a Service (PaaS), and Infrastructure as a Service (IaaS).[18] Each service is a type of "level" in the cloud, differentiated by the amount of control the user has over their information and how involved the cloud service provider is.[19] The SaaS level provides users access to web applications

---

14. PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING, SPECIAL PUBLICATION 800-145 (2011), http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf [https://perma.cc/X76X-2YDA] (archived Oct. 11, 2016) [hereinafter NIST].

15. GRACE LEWIS, BASICS ABOUT CLOUD COMPUTING, CARNEGIE MELLON UNIV.: SOFTWARE ENG'G INST. (Sept. 2010), http://resources.sei.cmu.edu/asset_files/WhitePaper/2010_019_001_28877.pdf [https://perma.cc/VYG4-HKXN] (archived Oct. 11, 2016).

16. ALEXA HUTH & JAMES CEBULA, U.S. DEP'T OF HOMELAND SECURITY, U.S COMPUT. EMERGENCY READINESS TEAM, THE BASICS OF CLOUD COMPUTING 1 (2011), https://www.us-cert.gov/sites/default/files/publications/CloudComputingHuth Cebula.pdf [https://perma.cc/HH68-XM4Z] (archived Oct. 11, 2016) (describing what the "cloud" is).

17. *See* Eric Griffith, *What Is Cloud Computing?*, PC MAG (May 3, 2016), http://www.pcmag.com/article2/0,2817,2372163,00.asp [https://perma.cc/5WWA-M4U4] (archived Nov. 1, 2016).

18. HUTH & CEBULA, *supra* note 16, at 2–3 (providing an overview of the three basics types of cloud service providers).

19. *See id.*; *see also* Narayanan, *supra* note 5, at 786 (describing briefly how each cloud service differs).

developed by third parties.[20] Examples include Google Apps and Web Outlook.[21] In this level, users have the least control over their data.[22] PaaS offers a space over the Internet where developers and other users can create their own applications and Web programs.[23] Finally, IaaS deals "with computational infrastructure" (e.g., storage, computation, and communications), meaning that the cloud service provider hosts the IT infrastructure of a user on its outside servers.[24] IaaS gives the user the most control over the cloud.[25] Overall, consumers are most likely to use SaaS models because applications are already developed, thus saving time and money. Meanwhile, businesses, including many small businesses, might be more inclined to use IaaS models because the models allow them to have as much computational capability as larger businesses without having to pay for the required physical infrastructure; the business only has to pay for the storage space and bandwidth used.[26]

All three services share five essential characteristics: on-demand self-service, broad network access, resource pooling, rapid elasticity, and measured service.[27] These characteristics give cloud computing "the illusion of infinite computing resources available on demand," but, in order to achieve this illusion, cloud service providers "must be able to move resources across servers as quickly and freely as possible."[28] For example, to achieve economies of scale, a cloud service provider might decide to process user data through a subcontractor, who might be located in a country different from both the service provider and user.[29] Furthermore, cloud service providers, in the quest to maintain high-speed services, might create more and more servers across a wider geographic area in order to maintain an efficient system.[30] While the cloud service provider is making all of these decisions behind the scenes, the user who has entrusted their data to the provider might not

---

20. LEWIS, *supra* note 15, at 2.

21. *Id.* (using Google Apps as an example of a Software as a Service capability).

22. *See* HUTH & CEBULA, *supra* note 16, at 3 (explaining the level of control over data the user has in each cloud service).

23. *Id.*

24. *Id.*

25. *Id.* (noting that the level of control increases from SaaS, to PaaS, to IaaS).

26. *Id.*

27. NIST, *supra* 14, at 2.

28. Narayanan, *supra* note 5, at 786–87.

29. *See Cloud Computing*, EUROPEAN DATA PROTECTION SUPERVISOR, https://secure.edps.europa.eu/EDPSWEB/edps/EDPS/Dataprotection/QA/QA10 (last visited Oct. 11, 2016) [https://perma.cc/726K-TTFV] (archived Oct. 11, 2016) [hereinafter EDPS] (explaining that in the context of cloud computing, the service provider makes many decisions regarding the processing of data, including but not limited to the use of sub-contractors); *see also* Narayanan, *supra* note 5, at 787 (describing how cloud service providers might join resources in order to take advantage of economies of scale).

30. Narayanan, *supra* note 5, at 787.

have any idea who is actually processing and storing their data, or where it is actually located, especially when using a SaaS provider.[31]

Global on-demand access to data and resource pooling are just some of the features of cloud computing that raise issues involving international law. From a data privacy perspective, the European Union has stricter laws regarding data privacy than the United States. Thus, companies must be cognizant of where and how EU user data is stored and processed, as compared to U.S. citizens' data. Indeed, the Microsoft case highlights how cloud computing's lack of physical borders raises international jurisdiction concerns due to differing approaches to law enforcement access.

B. *The Microsoft Case*

The Microsoft case illustrates the potential problems of cloud computing, especially when a party might find itself subject to the jurisdiction of multiple countries with opposing laws. Despite the Second Circuit's recent ruling, the issues brought up in the case are far from settled. In short, the case involves a warrant/subpoena, pursuant to the SCA, that compelled Microsoft to hand over the contents of an email stored on one of its foreign subsidiary's servers in Ireland in connection with a narcotics investigation. [32] The warrant issued required Microsoft to hand over all email data in its control, regardless of the data's stored location.[33] Based on the broad request, Microsoft filed for a motion to quash the warrant with respect to the user data stored in Ireland.[34] Many commentators have noted that the warrant did not offer any information as to the identity of the defendant, leading many to speculate that the subject of the investigation is a non-U.S. citizen.[35]

Microsoft argued before the Second Circuit that allowing this type of search would violate Ireland's sovereignty because the United States would essentially be conducting a search abroad without international

---

31. *See* Shamim Hossain, *Cloud Computing Basics*, THOUGHTS ON THE CLOUD (Feb. 4, 2014), http://www.thoughtsoncloud.com/2014/02/cloud-computing-basics/ [https://perma.cc/C7H6-RW73] (archived Nov. 1, 2016) (stating that generally consumers do not know where their data is processed, except for that fact that consumers may be able to specify where data is stored in some circumstances).

32. Brief for Appellant at 2, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 8, 2014).

33. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp. v. United States, 829 F.3d 197, 200–01 (2d Cir. 2016).

34. *Id.*

35. Orin Kerr, *A Different Take on the Second Circuit's Microsoft Case*, WASH. POST (Aug. 20, 2015), https://www.washingtonpost.com/news/volokh-conspiracy/wp/2015/08/20/a-different-take-on-the-second-circuits-microsoft-warrant-case/?utm_term=.afe6ea12b6ea [https://perma.cc/3THJ-GZV6] (archived Nov. 1, 2016).

cooperation.[36] Microsoft likened the stored data to documents located in a deposit box in a bank in Ireland.[37] The United States could not retrieve the deposit box contents without approval from Ireland.[38] Likewise, Microsoft argued that because the email data's "physical" location was in Ireland, the United States could not unilaterally gain access to the email contents.[39] The government and the magistrate judge who upheld the order both concluded that there was no extraterritorial application of the search warrant because the issue is who has control over the data; accordingly, they viewed the "physical" location of the data as irrelevant.[40] The magistrate judge also agreed that putting territorial restrictions on warrants issued under the SCA would greatly hamper the government's ability to investigate crimes.[41] Further, the magistrate judge addressed the argument that the government needed to issue the warrant pursuant to the Mutual Legal Assistance Treaty ("MLAT") with Ireland, which provides specific procedures each country must follow before executing a warrant abroad.[42] The judge stated that requiring the government to constantly refer to the MLAT process would also constrain law enforcement's ability to do its job.[43]

Ultimately, the Second Circuit held that the warrant could not compel Microsoft to hand over the user data held in Ireland.[44] Looking to both the plain meaning of the statute and its legislative history, the Second Circuit concluded that Congress did not intend for the SCA to apply extraterritorially.[45] Although the case is finished, the issues brought up are far from resolved. For instance, nothing is stopping another circuit court from finding that the SCA does allow extraterritorial warrants. Until Congress or the Supreme Court acts, the international issues surrounding cloud computing will continue to crop up.

---

36. Brief for Appellant at 3, Microsoft Corp. v. United States, No. 14-2985-cv (2d Cir. Dec. 8, 2014).

37. *Id.* at 1–4.

38. *Id.*

39. *Id.* at 18–19.

40. *See Microsoft Case*, *supra* note 6, at 472 (concluding that a subpoena under the SCA "requires the recipient to produce information in its possession, custody, or control regardless of the location of that information").

41. *Id.* at 474 ("[T]he burden on the Government would be substantial, and law enforcement efforts would be seriously impeded.").

42. *Id.* at 474–75.

43. *See id.* at 475 (noting that the MLAT process is "burdensome and uncertain").

44. *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d at 201.

45. *Id.* at 211 (noting that Congress did not give any affirmative indication in the legislative history to suggest the statute should apply extraterritorially).

C. *Principles of Jurisdiction in International Law*

An understanding of the foundational principles of jurisdiction in international law helps shed light on possible solutions to the problems posed by cloud computing. Principles of jurisdiction are important because they reflect how each country justifies its power to create and enforce its laws. No one seriously questions the ability of a state to create and enforce its laws within its own boundaries. However, when crafting laws that might have an unintended effect outside of the state's boundaries, or when making laws designed to purposefully stretch beyond those boundaries, reliance on a principle of jurisdiction is important to prevent diplomatic tensions. There are certain international principles, or norms, that countries observe if they seek to pass laws that might have what is called an extraterritorial effect. Thus, how a state justifies the exercise of its laws extraterritorially (i.e., beyond its own borders) can affect not only those residing within the country but also actors in the international community. Traditionally, there are five principles of international jurisdiction: the territorial principle, the nationality principle, the effects principle, the passive personality principle, and the protective principle.[46]

The *territorial principle* is the cornerstone of states' power to legislate, adjudicate, and enforce laws both domestically and internationally.[47] This concept supports states' power to make and enforce laws within their geographic region.[48] Generally, under this principle, a state is free to apply its laws to anyone, domestic or foreign, located within the state.[49] This principle is the least controversial form of jurisdiction in international law, and rarely leads to disputes.[50] However, over time, states have expanded this principle to exert

---

46. *See, e.g.*, AM. SOC'Y OF INT'L LAW, *Jurisdictional, Preliminary, and Procedural Concerns*, *in* BENCHBOOK ON INTERNATIONAL LAW II.A-2 (Diane Marie Amann ed., 2014), https://www.asil.org/sites/default/files/benchbook/jurisdiction.pdf (outlining the five basic principles governing the U.S. government's ability "to make its laws applicable to persons, conduct, relations, or interests"). One should note, however, that some sources classify the effects principle as a subset of one of the other principles and posit that the fifth principle is the universality principle, which focuses on conduct "recognized by the community of nations as of 'universal concern.'" *Id.* However, Section 402 the Restatement (Third) of Foreign Relations lists five bases of jurisdiction to prescribe and seemingly endorses the effects principle as its own bases of jurisdiction. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (AM. LAW INST. 1987). The Restatement does acknowledge the existence of universal jurisdiction, but notes that the principle is applied to exceptional offenses "such as piracy, slave trade, attacks on or hijacking of aircraft, genocide, war crimes, and perhaps certain acts of terrorism..." RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 404 (AM. LAW INST. 1987).

47. ANTHONY AUST, HANDBOOK OF INTERNATIONAL LAW 43 (2d ed. 2010).

48. Narayanan, *supra* note 5, at 790.

49. AUST, *supra* note 47, at 43.

50. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. c (AM. LAW INST. 1987)

jurisdiction over people or entities abroad if they have sufficient contacts with the state.[51]

The scope of the principle is ostensibly based on geography and physical borders.[52] However, based on each country's interests and customs, this principle can be expanded to give domestic laws extraterritorial effect, even if courts state that a law is not being applied extraterritorially.[53] This creates a certain irony in the international context, and different views regarding the breadth of the territorial principle can give rise to heated debates.[54] While this tension between competing views on the scope of the territorial principle has always existed in some form for decades, the rise of cloud computing exacerbates the tension because the data and technology are more ephemeral than the static concept of physical borders.

The *nationality principle*, also called the active personality principle, entitles a state to exercise its jurisdiction over its nationals, whether they are located at home or abroad.[55] This principle is recognized by the Restatement (Third) of Foreign Relations Law (the Restatement) in Section 402, which lays out the various bases for the jurisdiction to prescribe.[56] The nationality principle has naturally been rooted in the concept that the state has the authority to exert power over a specific group of people (e.g., a specific nationality), wherever located.[57] Historically, this has been uncontroversial; however, multinational corporations do not fit in this traditional basis for jurisdiction.[58] With the increase in companies that offer cloud computing services, which operate on servers across the globe, difficulties arise when trying to determine which state has jurisdiction.[59] For example, if it can be determined that states have concurrent jurisdiction over the same cloud computing provider, which

---

51. AUST, *supra* note 47, at 43.

52. *See id.* at 44.

53. CEDRIC RYNGAERT, JURISDICTION IN INTERNATIONAL LAW 50 (2008) (noting that competing normative views may give rise to different interpretations by countries, thus creating more problems than the "basic" principle would suggest).

54. *Id.*

55. AUST, *supra* note 47, at 44–45.

56. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (AM. LAW INST. 1987) ("Subject to § 403, a state has jurisdiction to prescribe with respect to . . . the activities, interests, status, or relations of its nationals outside as well as within its territory . . . .").

57. RYNGAERT, *supra* note 53, at 91.

58. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 414 cmt. a (AM. LAW INST. 1987) ("This section reflects the recognition that multinational enterprises do not fit neatly into the traditional bases of jurisdiction, [under] § 402.").

59. *See Gartner Says Physical Location of Data Will Become Increasingly Irrelevant in Post-Snowden Era*, GARTNER (July 2, 2014), http://www.gartner.com/newsroom/id/2787417 [https://perma.cc/FK2Y-3PAV] (archived Oct. 17, 2016) (discussing the future problems with data location and sovereignty).

jurisdiction must the provider comply with if the jurisdictions have conflicting laws? [60]

The *effects principle* has a somewhat murkier definition in international law, although it is conceptually similar to the nationality principle discussed above.[61] The principle grants a state jurisdiction over persons, entities, or activities that have a substantial effect within the state's territory, even if the person, entity, or activity is outside the state's territory.[62] For example, in the United States, this principle is applied to foreign subsidiaries of U.S.-based companies.[63] Even if the subsidiary is incorporated in a foreign country, the subsidiary is still subject to U.S. laws because of the United States' belief that a foreign subsidiary still has a large enough effect within the United States.[64] This exercise of jurisdiction has become increasingly controversial as a foreign subsidiary can be subject to competing, sometimes countervailing, state laws. [65] As mentioned above, this poses a dilemma, especially if each state has opposing economic laws and the company, in complying with one set of laws, is forced to ignore the other state's laws.

The *passive personality principle*, applied mostly in the criminal context, establishes state jurisdiction over any act committed by a person outside the state's territory if the victim of the act is a national of the state.[66] Under this principle, a state would have jurisdiction even if the person who committed the act was not a national of the state. [67] Some commentators have described this as "the most aggressive basis for extraterritorial jurisdiction."[68] As the Restatement notes, "[t]he principle has not been generally accepted for ordinary torts or crimes." [69] For instance, today, the passive personality principle has been used to justify the jurisdiction of U.S. laws over terrorists and other organized attacks committed against U.S. nationals abroad.[70]

---

60. *See* THE CHERTOFF GROUP, LAW ENFORCEMENT ACCESS TO EVIDENCE IN THE CLOUD ERA 13 (2015) [hereinafter CHERTOFF GROUP] (discussing the legal problems for service providers in today's world).

61. *See* AUST, *supra* note 47, at 45.

62. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 (AM. LAW INST. 1987).

63. *See* AUST, *supra* note 47, at 47.

64. *But see id.* (noting that the United States recognizes the effects principle when applying antitrust laws).

65. *Id.*

66. *See* RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. g (AM. LAW INST. 1987).

67. *Id.*

68. *See* RYNGAERT, *supra* note 53, at 92.

69. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402 cmt. g (AM. LAW INST. 1987).

70. *See id.*; *see also* AUST, *supra* note 47, at 44 (discussing the current applications of the passive personality principle).

The *protective principle* supports jurisdiction with respect to "certain conduct outside [a state's] territory by persons not its nationals that is directed against the security of the state or against a limited class of other state interests."[71] Examples of conduct that generally fall within this principle include "espionage, counterfeiting of the state's seal or currency, falsification of official documents, . . . and conspiracy to violate the immigration or customs laws."[72] The United States or the European Union would probably not apply the protective principle to laws covering cloud service providers since states reserve the use of the protective principle for only a small set of crimes.[73]

In the end, states can rely on any one of these principles when drafting laws to enable law enforcement to access certain cloud computing data abroad. Whether or not other states will accept the use of any one of these principles is another matter. Furthermore, states do not even apply the principles in the same way, as will be discussed below. All of this leads to a problem of uncertainty for cloud computing service providers who might be unsure how each country will apply their laws. Therefore, when it comes to providing for law enforcement access to cloud data, a common approach must be taken to ensure stability and certainty. What that approach is, and whether it will work, will be discussed further in Part IV.

III. A COMPARATIVE LOOK AT THE UNITED STATES AND UNITED KINGDOM

This Part will compare the primary law in the United States dealing with law enforcement access to cloud data, the SCA, with the analogous law in the United Kingdom, the Regulation of Investigatory Powers Act 2000. This comparison, while limited to only the United States and United Kingdom, is meant to illustrate that the issue with the cloud is not relegated to only the United States—other countries might soon find themselves dealing with their own Microsoft case. The comparison will also show that the many myths about the United States' allegedly broad, unilateral access to data around the globe are misconceived.[74] For instance, the United Kingdom's laws regarding

---

71. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 402(3) (AM. LAW INST. 1987).

72. *Id.* cmt. f.

73. *See* RYNGAERT, *supra* note 53, at 98 (stating that protective jurisdiction is hardly exercised in the real world).

74. *See generally Should governments be able to look at your data abroad?*, ECONOMIST (Sept. 8, 2015), http://www.economist.com/news/business-and-finance/21663902-test-case-set-determine-whether-fbi-can-access-microsofts-foreign-data-should [https://perma.cc/95FU-PCV9] (archived Oct. 17, 2016) (noting the possible broad powers the U.S. government possesses).

law enforcement access to cloud data potentially grant UK law enforcement similarly broad powers. Both laws are silent on the applicability of any extraterritorial powers. The drafters did not, and likely could not, foresee the rise in cloud computing. However, how each country presently justifies the extraterritorial application is a matter of grave importance for citizens, corporations, and other countries.

A. *U.S. Law Enforcement Access to the Cloud*

The Electronic Communications Privacy Act ("ECPA"), passed in 1986, lays out the statutory framework that U.S. law enforcement must follow when accessing electronic information.[75] Title II of the ECPA, the SCA, currently governs the mandatory disclosure of data held by cloud providers to law enforcement officials.[76] The SCA provides that third-party Internet service providers ("ISPs") must disclose customer data to the government, as long as the government goes through one of three legal mechanisms provided in the statute.[77] Depending on the method used, the government will have to satisfy a specific legal standard before obtaining authorization to compel an ISP to turn over customer data.[78] Also, depending on whether the data has been stored for more than 180 days or not, the government must follow certain procedures.[79]

Law enforcement can only require ISPs to disclose customer information stored for 180 days or fewer if they apply for a search warrant pursuant to the Federal Rules of Criminal Procedure.[80] If the government applies for a search warrant, it must show a judge that probable cause exists for the disclosure of the customer's data.[81] This route provides the most protection to customers when it comes to keeping their data private because probable cause is a high bar for the government to meet, and it must be done before a judicial officer.[82]

---

75. *See Electronic Communications Privacy Act (ECPA)*, ELECTRONIC PRIVACY INFORMATION CENTER), https://epic.org/privacy/ecpa/ (last visited Nov. 1, 2016) [https://perma.cc/73AF-XXAU] (archived Nov. 1, 2016) (providing an overview of the ways the ECPA allows law enforcement to access electronic records).

76. Reema Shah, Comment, *Law Enforcement and Data Privacy: A Forward-Looking Approach*, 125 YALE L. J. 543, 545 (2015)

77. *See* WINSTON MAXWELL & CHRISTOPHER WOLF, A GLOBAL REALITY: GOVERNMENTAL ACCESS TO DATA IN THE CLOUD 4 (May 23, 2012), http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf [https://perma.cc/487Y-9U2W] (archived Oct. 17, 2016).

78. 18 U.S.C § 2703 *et seq.* (2012)

79. 18 U.S.C § 2703 (a) (2012)

80. *Id.*

81. *Id.*; *see also* MAXWELL & WOLF, *supra* note 77, at 4 (discussing the legal mechanism of the SCA).

82. Orin Kerr, *What Legal Protections Apply to E-mail Stored Outside the U.S.?*, WASH. POST (July 7, 2014), https://www.washingtonpost.com/news/volokh-conspiracy/

However, for data that is stored for over 180 days, the government must produce either a subpoena or court order.[83] With regards to a subpoena, the government need only establish that it has "reasonable grounds to believe that the contents are relevant to a criminal investigation."[84] The reasonable grounds standard is easier to prove than probable cause.[85] When the government seeks a court order, the SCA requires the government to establish "specific and articulable facts" showing that it has reasonable grounds to believe the electronic data will be helpful to the investigation.[86] This standard is essentially the same as the one for obtaining a subpoena.[87]

Despite this lower standard, the SCA provides an additional protection to cloud service customers if the government seeks a court order or subpoena. Before accessing the stored data, the government must give prior notice to the customer.[88] However, prior notice does not have to be given if the government can show that providing prior notice might endanger the life of an individual, increase the risk of flight from prosecution, increase the risk of tampering with evidence, or otherwise seriously jeopardize an investigation or trial.[89] Furthermore, prior notice does not need to be given to the customer if the government's request is in the form of a traditional warrant.[90] Because the government can argue that revealing its request will hamper its investigation, the protection of prior notice might not have any real "teeth" when it comes to protecting consumer information stored in the cloud.

Despite these legal mechanisms, the SCA is outdated when it comes to recognizing current electronic communication and defining the scope of protections for consumer data. For example, the SCA requires the government to use one of the legal mechanisms mentioned above depending on whether the information sought is kept by an electronic communications service ("ECS") or by a remote computing service provider ("RCS").[91] An ECS is defined as "any service, which provides users thereof the ability to send or receive wire or electronic communications."[92] Whereas a RCS is defined as "the provision to the

---

wp/2014/07/07/what-legal-protections-apply-to-e-mail-stored-outside-the-u-s/ [https://perma.cc/GF9U-7LD5] (archived Oct. 17, 2016) (comparing the legal standards of a traditional warrant versus a subpoena).

83. 18 U.S.C § 2703(b)(1)(B)(i) and (d).
84. Shah, *supra* note 76, at 545.
85. *See id.* (noting that "reasonable grounds" is a lower standard than probable cause).
86. 18 U.S.C § 2703(d).
87. Shah, *supra* note 76, at 545.
88. 18 U.S.C. § 2703(b)(1)(B).
89. 18 U.S.C. § 2705.
90. 18 U.S.C. § 2703(b).
91. *Microsoft Case*, *supra* note 6, at 469 n.2.
92. 18 U.S.C. § 2510(15).

public of computer storage or processing services by means of an electronic communication system."[93] However, as the magistrate judge in the Microsoft case noted, "[s]ince service providers now generally perform both functions, the distinction, which originated in the context of earlier technology, is difficult to apply."[94] Likewise, the line drawn between requests for data stored more than 180 days and data that has been stored for less than that is increasingly irrelevant and arbitrary.[95] In today's world, data is routinely kept longer than 180 days, such that the distinction in the statute has become meaningless.[96]

As the Microsoft case has shown, the biggest drawback to the SCA is its silence on its extraterritorial application and the outer limits on the government's ability to compel ISPs to turn over consumer data. As already discussed, much of the case hinged on whether or not the statute applies to controllers of the information, based on their location, or whether the statute applies to the physical location of the data itself.[97] While the Second Circuit has found that the SCA does not apply extraterritorially, the SCA's silence on the matter allows other circuits to develop opposing interpretations.

Since the start of the Microsoft case in 2014, many commentators and foreign politicians have expressed concern over the U.S. government's unfettered power to access data stored anywhere in the cloud across the globe.[98] The SCA provides for certain procedures that actually protect consumers' information. For example, the SCA requires that the government show specific facts to a judicial officer before compelling an ISP to hand over consumer data.[99] While the standard might be low, a standard must still be met. However, fears over the scope of the SCA are somewhat founded considering the global nature of the Internet today and the SCA's complete silence on the issue of territoriality. While not perfect, the SCA has analogues in other countries, including European countries, despite the fact the European Union has been critical of the SCA and the Microsoft case.[100]

---

93. 18 U.S.C. § 2711(2).

94. *Microsoft Case*, *supra* note 6, at 469 n.2.

95. *See id.*

96. *See* Shah, *supra* note 76, at 545 ("The distinctions drawn in the ECPA between communications stored for more or less than 180 days are vestiges of a bygone era.").

97. *Id.*

98. Sam Thielman, *Decision in Microsoft case could set dangerous global precedent, experts say*, GUARDIAN (Sept. 9, 2015 7:00 PM), https://www.theguardian.com/technology/2015/sep/09/microsoft-federal-case-data-security-precedent [https://perma.cc/ZV8S-Z66X] (archived Oct. 17, 2016) (summarizing the reaction of many commentators on the potential power of U.S. law enforcement).

99. 18 U.S.C. § 2703(d).

100. Letter from Viviane Reding, Vice President of Justice, Fundamental Rights, and Citizenship, European Commission, to Sophie in 't Veld, Member of the European Parliament (June 24, 2014) (http://www.nu.nl/files/nutech/Scan-Ares-MEP-in%27t-Veld-

B. *UK Law Enforcement Access to the Cloud*

Many European countries have derided the United States for its seemingly broad data interception powers.[101] This would lead one to think that European countries have laws that respect and take seriously the concept of digital privacy. The European Union does in fact take seriously the right of every citizen to data privacy.[102] Yet many EU members have their own domestic laws regarding data collection that are effectively similar to the powers given to the U.S. government by the SCA.[103] Currently, the main statute in the United Kingdom that deals with data collection, and cloud data collection specifically, is the Regulation of Investigatory Powers Act 2000, or "RIPA."[104] An analysis of RIPA's main sections reveals that the UK government's ability to intercept cloud data is not only similar to the U.S. government's, but also that RIPA causes many of the same problems that the SCA does when it comes to the treatment of data stored in the cloud.

Much like the SCA, RIPA starts out with the broad law that it is illegal to intercept any communication without lawful authority in the United Kingdom.[105] However, the statute then goes on to describe if and when there are lawful interceptions of communications. Underpinning RIPA is the distinction between the terms "interception" and "communications data."[106] This distinction is important because it affects the way in which the government's powers can be used.[107]

"Interception" takes place when "the contents of the communication [are made] available, while being transmitted, to a person other than the sender or intended recipient of the communication."[108] The term "content" is not defined, but it includes

---

.pdf [https://perma.cc/UR7G-EVXV] (archived Nov. 1, 2016)) (expressing the view that the extraterritorial application of the SCA might be in violation of international law).

101. *See* Kendrick, *supra* note 13 (discussing the outrage some European have over US law enforcement capabilities).

102. Charter of Fundamental Rights of the European Union art. 8, 2000 O.J. C 364/01 [hereinafter Charter of Rights] (indicating that "[e]veryone has a right to the protection of personal data concerning him or her").

103. *See, e.g.*, Regulation of Investigatory Powers Act 2000, c. 1 (Eng.) [hereinafter RIPA].

104. CLIVE GRINGAS, UK CLOUD COMPUTING INTERCEPTION – NOTHING NEW 2 (2011) http://www.olswang.com/pdfs/CloudComputingInterception_CQG.pdf [https://perma.cc/9FZN-RFN9] (archived Oct. 17, 2016).

105. *Compare* RIPA, c. 1, § 1(a) *with* 18 U.S.C. § 2701(a).

106. DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW 95, ¶ 6.5 (2015) https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/434399/IPR-Report-Web-Accessible1.pdf [https://perma.cc/U2JC-S74K] (archived Oct. 17, 2016) [hereinafter UK INVESTIGATORY POWERS REPORT].

107. *Id.* at ¶ 6.2.

108. RIPA, c. 1, § 2(2).

everything from the actual content of the electronic communication, like a text message, to the metadata, such as when the message was sent.[109] Strikingly, the government has also classified a Google search as a type of communication.[110] Of equal importance is how the law defines when a communication is being transmitted. According to RIPA:

> [T]he times while a communication is being transmitted by means of a telecommunication system shall be taken to include any time when the system by means of which the communication is being, or has been, transmitted is used for storing it in a manner that enables the intended recipient to collect it or otherwise to have access to it.[111]

This definition of "transmission" is important because it has been interpreted to mean that voicemails stored on a phone are "in the course of transmission."[112] This principle applies with equal force to emails stored on a third-party server.[113] Therefore, depending on the statutory authorizations needed, emails stored on a server somewhere can be accessed or "intercepted" by UK law enforcement, provided all other conditions are met.

"Communications data," meanwhile, excludes the content of communications, and consists of a more limited range of information. Generally, RIPA defines "communications data" as "data about use made of a telecommunications or postal service, but not the contents of the communications themselves."[114] The statute lists three main categories of communications data: traffic data (such as cell-site data and certain types of IP addresses); service use information relating to the use of a particular service (e.g., itemized phone bill); and subscriber information, which includes any information that a user hands over to the service provider (e.g., email address, name, and other personal information required to sign up).[115] People familiar with the "Snowden leaks" might recognize that "communications data" under RIPA is similar to the term "metadata" that has caused much controversy in the United States.[116]

---

109. RICHARD KEMP, CLOUD COMPUTING AND DATA SOVEREIGNTY 14 (2015) http://www.kempitlaw.com/wp-content/uploads/2015/10/Cloud-Computing-and-Data-Sovereignty.pdf [https://perma.cc/XYM8-KDY8] (archived Oct. 17, 2016).

110. *See* UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 108 ¶ 6.52 (commenting on how a Google search is considered communications data).

111. RIPA, c. 1 § 2(7).

112. *Edmonson, Weatherup, Brooks, Coulson & Kuttner v. R* [2013] EWCA Crim 1026 (appeal taken from Eng.).

113. UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 95 ¶ 6.5.

114. *Id.* at 96, ¶ 6.6.

115. RIPA, c. 2, § 21(4); *see also* UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 96, ¶ 6.6.

116. *See generally* Robert Pritchard, *Update Our Legislation on Data and Security*, RUSI (Oct. 31, 2013), https://rusi.org/commentary/snowden-leaks-need-update-

With regards to the interception of communication content, RIPA governs which agencies have the power to intercept data and how broad their powers are. The use of the interception warrants is limited to MI5, MI6, the Government Communications Headquarters (GCHQ), the National Crime Agency (NCA), the Metropolitan Police Service, the Police Service of Northern Ireland and Scotland, Her Majesty's Revenue and Customs, and the Ministry of Defence.[117] Any other agency looking to use an interception warrant, or any oversees agency seeking one through a mutual legal assistance treaty (MLAT), must request one of these agencies to apply on their behalf.[118] However, according to the British government, it is rare for a MLAT request to be filed or authorized, supporting the U.S. government's pessimistic view of the MLAT process.[119]

An authorization under RIPA is achieved once two requirements are met. First, the warrant sought must be "in the interests of national security, for the purpose of preventing or detecting serious crime[,] for the purpose of safeguarding the economic well-being of the United Kingdom," or to give effect to any international mutual assistance agreement.[120] Second, the secretary of state must believe that the interception of communications is necessary and proportionate to the objective sought.[121] This limit is put in place to respect the European Union's law regarding citizens' right to data privacy, as laid out in the Article 8 case law of the ECtHR.[122]

Interception warrants come in two forms: targeted warrants or bulk warrants. According to Article 8, targeted warrants must involve a specific person whose communications will be intercepted or a single location.[123] According to British officials, these target warrants may authorize the interception of electronic communication (e.g., communications stored in the cloud) between two people in the British Islands or two people communicating overseas.[124] Meanwhile, bulk warrants, or external warrants, authorize British law enforcement to intercept communications that are outside of the British Islands.[125] Specifically, these warrants allow British law enforcement to intercept

---

our-legislation-data-and-security [https://perma.cc/TA3N-QVZK] (archived Nov. 1, 2016) (discussing how the evolution of metadata implicates the need to update RIPA, especially after the Edward Snowden's revelations).

117. UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 104, ¶ 6.38.

118. *Id.* at 104, ¶ 6.39.

119. *Id.*

120. RIPA, c. 1, § 5(3); KEMP, *supra* note 109, at 14.

121. UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 103, ¶ 6.37.

122. *Id.* at 104, ¶ 6.37.

123. RIPA, c. 1, § 8; *see also* UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 104 ¶ 6.42.

124. *Id.* at 105, ¶ 6.43.

125. *Id. at* ¶ 6.45.

large volumes of data either carried on fiber optic cables or carried by a specific service provider.[126]

The current British laws regarding the access to "communications data" are in flux due to recent rulings by the High Court.[127] Previously, electronic service providers were required by law to maintain records of all users' communications data for at least a year.[128] Whether the rule will remain in place is uncertain at the moment. What is known, though, is that RIPA is less restrictive about law enforcement's access to communications data. Compared to the limited number of agencies that could apply for interception warrants, roughly six-hundred agencies can seek access to a user's communications data. [129] Furthermore, the reasons for applying for the warrant can be broader.[130]

Despite RIPA having been passed almost twenty years after the SCA's enactment, it too has issues dealing with the rise in cloud computing and the global nature of the Internet. This has not gone unnoticed by some officials within the British government who have recognized that data in the possession of overseas services presents "unique jurisdictional challenges when UK law enforcement agencies wish to gain access to [that] data."[131] The British Parliament passed the Data Retention and Investigatory Powers Act 2014 (DRIPA), which amended and addressed the extraterritorial effect of warrants issued under RIPA.[132]

For interception warrants, a person (or service provider) is required to comply with such a warrant whether or not the person is located in the United Kingdom.[133] The person is not required to take steps that are not reasonably practicable, and the person does not have to take steps that might cause them to violate the laws of another country. [134] Furthermore, under the recently amended RIPA, the secretary of state may require anyone providing public telecommunications services to assist with an interception warrant, irrespective of whether or not the provider is in the United Kingdom.[135] The effect might be quite similar to that of the SCA because the cloud

---

126. *Id.*

127. *See* KEMP, *supra* note 109, at 13 (discussing the statutory history of the most recent RIPA provisions).

128. *Id.* at 15.

129. *Id.*

130. *See* UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 111, ¶ 6.64 (describing differences between interception warrants and communications data warrants).

131. *Id.* at 118, ¶ 6.95.

132. *Id.*

133. RIPA, c. 1, § 11(4).

134. *Id.* §11 (5).

135. RIPA, c. 1, § 12.

computing service provider might find itself compelled to comply with a warrant simply because it transmitted user data subject to UK law.

As amended, RIPA seems to suggest that if a company providing cloud computing services in the United Kingdom, such as Microsoft, Google, or Amazon, was provided with one of these interception warrants, cloud computing service providers would be required to take certain reasonable steps to comply with, and possibly hand over content data to, UK law enforcement. In regards to communications data, UK law enforcement can probably require a person or service provider to provide access to said data, irrespective of the operator's location, so long as it is reasonably practicable.[136]

To date, there have been no cases dealing with this issue of enforcing these obligations on a service provider overseas.[137] However, it is not a stretch of the imagination to see how these provisions could give rise to a case similar to the Microsoft case in the United States. For instance, UK law enforcement might take a similar stance regarding oversees data as U.S. law enforcement did in the Microsoft case. In that case, U.S. law enforcement believed it was reasonable for Microsoft to hand over overseas communications because Microsoft could access the data from its U.S. offices. UK law enforcement or the secretary of state might also think it is reasonable that a public service provider with an UK office could retrieve overseas data if it was legal in the United Kingdom. It is uncertain if the United Kingdom will follow the same path as the United State. However, from this comparison, it is clear that the United States is not unique in its approach to law enforcement access to electronic communications.

IV. A TWO-PRONG APPROACH TO ADDRESSING THE ISSUE

This Part will discuss possible solutions to the problem that the cloud poses in the context of law enforcement access. First, much has been said about fixing "uncertainty" and providing "stability," but this Part will explain in more depth why these issues must be resolved. Second, this Part will argue for a two-prong approach to solving the issue of law enforcement access concerning the cloud—with a focus on both a common understanding of which principle of jurisdiction should be applied in this context and the reforming of the MLAT system.

---

136. *See generally* UK INVESTIGATORY POWERS REPORT, *supra* note 106, at 119, ¶ 6.99 (observing that no case has tested the full extraterritorial effect of RIPA).

137. *Id.*

A. *The Consequences if Nothing Is Done*

Currently, U.S. companies account for over half of the cloud computing industry.[138] In 2014, companies spent $72 billion on cloud computing services globally.[139] However, this state of affairs might not last long if there is no solution to harmonize or more clearly define the jurisdictional boundaries of the laws of the United States and other countries. Since Edward Snowden revealed the National Security Agency's surveillance practice, cloud computing providers have faced increasing pressure from European governments to keep the data of European citizens out of the United States, and instead to "localize" the data in each European country.[140] The result is that cloud computing providers have been busy building more and more data centers in Europe.[141]

This movement, dubbed "data localization,"[142] is troubling and would undermine the main benefits of cloud computing.[143] First, if cloud service providers start housing user data in regional data centers, this would prevent cloud service providers from achieving efficient economies of scale. As mentioned earlier, cloud computing works because it allows service providers the ability to pool resources from processors across the globe in order to achieve efficient economies of scale and meet consumer demand during peak usage times.[144] Besides restraining cloud computing from achieving its full potential, other commentators have protested about more than just the negative economic losses, positing that "[t]he very nature of the World Wide Web

---

138. James Bourne, *AWS, Microsoft, IBM and Google "leave rest behind" in cloud infrastructure market*, CLOUD TECH. (July 24, 2015 00:12 AM), http://www.cloudcomputing-news.net/news/2015/jul/24/aws-microsoft-ibm-and-google-leave-rest-behind-cloud-infrastructure-market/ [https://perma.cc/S234-PKGQ] (archived Oct. 17, 2016).

139. INTERNATIONAL TRADE ADMINISTRATION, DEPARTMENT OF COMMERCE, 2015 TOP MARKETS REPORT: CLOUD COMPUTING 3 (2015) http://trade.gov/topmarkets/pdf/Cloud_Computing_Top_Markets_Report.pdf [https://perma.cc/7TPG-PTJZ] (archived Oct. 17, 2016).

140. Paul Roberts, *In wake of Snowden, U.S. cloud providers face calls to wall off data*, IT WORLD (Jan. 27, 2014), http://www.itworld.com/article/2699656/security/in-wake-of-snowden--u-s--cloud-providers-face-calls-to-wall-off-data.html [https://perma.cc/JH38-W2YM] (archived Oct. 17, 2016).

141. *See, e.g.*, Lisa Fleisher, *Apple Spending Nearly $2 Billion on European Data Centers*, WALL ST. J. (Feb. 23, 2015 8:07 AM) http://www.wsj.com/articles/apple-to-invest-1-9-billion-in-european-data-centers-1424685191 (subscription required) [https://perma.cc/8FNS-Z7P9] (archived Oct. 17, 2016).

142. Anupam Chander & Uyen P. Le, *Breaking the Web: Data Localization vs. the Global Internet* 3–4 (Univ. of Cal., Davis Sch. of Law, Research Paper No. 378, 2014).

143. *Id.* ("[D]ata localization increases the ability of governments to *surveil* and even oppress their own populations.").

144. *See* Hossain, *supra* note 31 (citing resource pooling and rapid elasticity as basic traits of all cloud computing services).

is at stake" and that a continued push for data localization laws will "break up the World Wide Web."[145]

However, this move to localize data would not allay any concerns Europeans might have regarding U.S. surveillance practices unless clear jurisdictional lines were laid out. As will be discussed below, the United States applies different principles of jurisdiction to give its laws extraterritorial effect than do European countries, such as the United Kingdom. Thus, localizing data would not protect data stored on a Microsoft server in Germany if the United States applied its broad view of the nationality principle, or the effects principle, to Microsoft. Therefore, a common approach to defining the jurisdictional basis of laws relating to law enforcement access must be taken in order to promote a free-flowing trade of information and services, and to ensure the continued growth of the cloud computing industry instead of cutting it off.

B. *Prong One: Using the Principles of Jurisdiction to Refocus the Issue*

A big part of the debate surrounding law enforcement access to cloud data is each country's unique perspective and public policy in applying laws extraterritorially. As the discussion above showed, on the books, both the SCA and RIPA seem to leave open the prospect that law enforcement can access data on the cloud, even if the data is located in another country.[146] However, while many criticize the United States for its position in the Microsoft case, less attention is given to the fact that RIPA gives law enforcement in the United Kingdom similar powers. [147] Thus, how each country has traditionally applied international jurisdiction principles is important in determining the potential extent of law enforcement access and whether a common perspective can be adopted.

How far states stretch their view of the territoriality principle depends on their respective culture and the overall interests they wish to advance.[148] For example, the United States and many European countries view the territoriality principle as a possible justification for orders of discovery abroad.[149] The current debate and concern around the Microsoft case is a perfect example of these two differing views. For instance, according to the magistrate judge in the Microsoft case, the fact that Microsoft is domiciled in the United States, and has access to

---

145. Chander & Le, *supra* note 142, at 4.

146. See infra, Part III.

147. *But see* CHERTOFF GROUP, *supra* note 60 (reporting on the similarities between the powers granted by the SCA and similar laws in other countries).

148. *See* RYNGAERT, *supra* note 53, at 79 (discussing the different approaches European countries and the United States take under the territoriality principle in the context of acquiring foreign based evidence).

149. *Id.*

data stored abroad, allows for the application of the SCA without any extraterritorial application.[150]

Indeed, the United States' approach to handling discovery requests for law enforcement access is decidedly more unilateral than other countries.[151] The Restatement even recognizes this difference in the reporter's comments to Section 442, noting: "[n]o aspect of the extension of the American legal system beyond the territorial frontier of the United States has given rise to so much friction as the request for documents associated with investigation and litigation in the United States."[152] While this broad view seems to conflict with the territoriality principle, as the United States is applying its discovery requests outside of its natural territory, the United States' view is that the "main acts" of document production are taking place exclusively within the United States.[153] In theory, U.S. discovery requests abroad would only violate the territoriality principle if law enforcement agents sought to enforce these requests within the borders of foreign territories.[154]

Meanwhile, many European countries resort to international cooperation when it comes to discovery orders for documents located abroad.[155] As a result, this approach does not give rise to many concerns in the international context and seems to follow a stricter interpretation of the territoriality principle when applied to European rules of discovery.[156] Thus, perhaps one reason for the issue of UK law enforcement access to data stored abroad might be because of this cooperative approach.

Both the SCA and RIPA are based on the principle of territoriality because they place certain obligations on service providers that reside within their country, regardless of whether or not the service provider is a domestic national or a foreign national.[157] However, using the physical location of the service provider as the "jurisdictional hook" of these laws creates the problems currently playing out in the Microsoft case.[158] Therefore, one solution is to redefine how the statutes focus on territoriality. Instead of focusing on the company and its location, one solution would be to focus on the nationality of the user and where the content is produced, in essence using the nationality principle.[159]

---

150. *Microsoft Case*, *supra* note 6, at 474.
151. *Id.; see also* CHERTOFF GROUP, *supra* note 60, at 13.
152. RESTATEMENT (THIRD) OF FOREIGN RELATIONS LAW § 442 note 1 (AM. LAW INST. 1987).
153. *See* RYNGAERT, *supra* note 53, at 80.
154. *Id.*
155. *Id.*
156. *Id.*
157. *See generally* RIPA, c. 1.
158. *See* MAXWELL & WOLF, *supra* note 77, at 2–3.
159. Shah, *supra* note 76, at 550.

This approach would be beneficial for several reasons. From an economic perspective, it would ensure the continued growth of the cloud computing market worldwide, which would be a boon for the U.S. technology companies that currently dominate the market.[160] This is because the incentive for data localization—"requiring foreign companies to store citizens' data within a country's borders"[161]—would be greatly minimized.[162] Part of the rise in this movement for data localization is fueled by the desire of governments to protect their citizens' data from unwanted searches from foreign governments.[163] Thus, knowing that a citizen's nationality determined the effect of a law like the SCA or RIPA would give these countries peace of mind and lessen the motivations for data localization. This would also create more regulatory certainty for companies, thus decreasing any potential costs arising from the current murky legal environment. Another benefit is that this approach would still give U.S. and UK law enforcement the power to compel telecommunications providers to hand over data, whether it is stored at home or abroad, provided the data belongs to a national citizen or the data was created in their country.[164]

However, for data created by a foreign citizen, law enforcement would not have the power to compel service providers to give them access to the data. Instead, law enforcement would have to respect the MLAT process and request the help of a foreign nation.[165] This approach would fall in line with the traditional principles of international jurisdiction and comity.[166] As discussed above, traditionally, the territoriality principle recognizes that a state cannot enforce or execute a warrant outside of its boundaries.[167] This new approach would respect this principle because no country (whether it be the United States, United Kingdom, or another) would be allowed to retrieve the data, even if it could be retrieved from overseas in the home country, without seeking foreign assistance.[168] Relying on this framework and the MLAT process would acknowledge the sovereignty of the foreign citizens' government and respect its own principles. For instance, if the United States went through the MLAT process to

---

160. Elias Groll, *Microsoft vs. the Feds, Cloud Computing Edition*, FOREIGN POL'Y (Jan. 21, 2016) http://foreignpolicy.com/2016/01/21/microsoft-vs-the-feds-cloud-computing-edition/ [https://perma.cc/UR2J-7JTA] (archived Oct. 17, 2016) (reporting that four U.S. technology companies own nearly half the market currently).

161. *See* Kendrick, *supra* note 13.

162. *See* Shah, *supra* note 76, at 550.

163. *See id.* (describing how localization can hinder progress in cloud computing as one effect of existing incentives).

164. *Id.*

165. *Id.*

166. *Id.* at 551.

167. AUST, *supra* note 47, at 43.

168. *See* Shah, *supra* note 76, at 551.

retrieve the data of a French national, the United States would be respecting the basic fundamental right to data privacy that EU members all believe in.[169] Similarly, other countries would not be able to access the data of a U.S. citizen just because Microsoft has an office in another country—something that U.S. service providers already fear.[170] This approach would hopefully strengthen the norms of international sovereignty and comity to respect the right of each state to govern its own citizens. Furthermore, it can contribute to repairing the relationship between the United States and many European countries over the Snowden leaks and lessen the suspicion many countries currently harbor against the United States.[171] In return, other countries would hopefully respect the interests of the United States in maintaining its citizens' privacy.

Admittedly, there are several problems with this approach. One problem arises when law enforcement is unable to identify or trace the user of the data, due to the use of an anonymous IP address.[172] What should law enforcement do if they are unable to determine with absolute certainty the nationality of the user? Do they wait and possibly give up a lead due to their hesitation? Or does U.S. law enforcement proceed anyway in the hope that the user is a U.S. citizen? This problem might not be as grim as it sounds due to how sophisticated service providers now are with data location tracking.[173] Service providers most likely know where their user first created the data, so the uncertainty of the nationality of the user is probably low.[174] However, for the most sophisticated criminals, there is still the chance that they will be able to keep their location and nationality anonymous.[175]

Finally, a last problem with this approach is its reliance on the MLAT process. The current MLAT request process is extremely slow, which is one reason why the United States served the warrant on Microsoft instead of going through the MLAT process with Ireland.[176]

---

169. Charter of Rights, *supra* note 102, art. 8.

170. *See* Kendrick, *supra* note 13 (stating the concern U.S. companies have over new laws passed in Russia).

171. Shah, *supra* note 76, at 543 ("[F]oreign governments reacted forcefully to the revelations, effecting new laws and policies to shield information from the National Security Agency.").

172. *Id.* at 552.

173. *Id.*

174. *Id.*

175. *See id.* (mentioning that recent developments in law enforcement have made it harder for cyber criminals to remain anonymous).

176. *Microsoft Ireland Case: Can a US Warrant Compel a US Provider to Disclose Data Stored Abroad?* CENTER FOR DEMOCRACY & TECH. (July 30, 2014) https://cdt.org/insight/microsoft-ireland-case-can-a-us-warrant-compel-a-us-provider-to-disclose-data-stored-abroad/ [https://perma.cc/Q73N-RTAC] (archived Oct. 17, 2016) (summarizing the Justice Department's argument that MLAT's are "too slow and cumbersome to be adequate alternatives").

Simply suggesting to focus on the identity of the user or place of data creation, without also reforming the MLAT system, is to offer a somewhat utopian, and most likely ineffective solution. Without any MLAT reform, countries will have no incentive to change their ways because the MLAT process is too slow for law enforcement to effectively do its job. Thus, all that will be left is countries making empty promises and false words about respecting state sovereignty, while covertly law enforcement uses other means to acquire the sought after data.

Unless there is a binding treaty or other document to hold each country accountable to focusing on the nationality of the user, there will be nothing stopping countries from going back on their promises, except perhaps shame in the international community. As was discussed above, countries take widely different views on how to interpret and apply these principles. Who is to say how a country will interpret the principle regarding a focus on the nationality of the user? Thus, reforming the MLAT process is critical so that countries feel less desire to "cheat" and liberally expand the principle to suit their needs. What MLAT reform must do, and how it could work, will be discussed below in the next Section.

Other authors have suggested that using other principles of international jurisdiction might solve some of the problems posed by the cloud. For example, some have written about applying the nationality principle to the cloud service providers.[177] Applying the nationality principle to statutes like the SCA and RIPA would not serve as a silver bullet to the problem of law enforcement access to cloud data. Defining a corporation's "nationality" is difficult because it depends on the frame of reference one takes. A corporation's nationality can be different depending on whether the nationality is based on the state of incorporation, majority shareholder nationality, or other links to the forum.[178] Another issue is raised when a state attempts to impose its laws on a foreign entity simply because the foreign entity is a subsidiary of a corporation located within the state.[179] Under U.S. practice, nationality is determined by the state that the corporation is incorporated in.[180] Furthermore, the United States recognizes that foreign subsidiaries of national corporations fall under U.S. law.[181] Thus, from a U.S. perspective on the nationality principle, the concept of *control* can be crucial in determining the scope of its jurisdiction to prescribe and enforce its laws. This principle of control is once again illustrated in the Microsoft case.[182]

---

177. Narayanan, *supra* note 5, at 796.
178. RYNGAERT, *supra* note 53, at 91.
179. *Id.*
180. *See* Narayanan, *supra* note 5, at 796.
181. *Id.*
182. *See Microsoft Case*, *supra* note 6, at 472 (emphasizing that subpoenas have always been about the control by the recipient, and not where the content is located).

Applying this nationality principle to corporations that offer or use cloud computing would lead to several issues. One is that currently, U.S. corporations dominate the global cloud computing market.[183] Therefore, most of the cloud computing industry must comply with both U.S. law and the domestic laws of the countries in which businesses operate.[184] Taken to the extreme, applying this nationality-control principle to cloud computing service providers would cause serious problems for businesses seeking to comply with regulations abroad, for example, Europe's strict data protection regime.[185] Thus, an approach that relies on focusing on the service provider's nationality is unlikely to serve as an effective solution, especially if a service provider finds itself falling under the jurisdiction of two countries that have opposing laws.

Another principle that might be used to justify the extraterritorial application of law enforcement access statutes is the passive personality principle.[186] Although, applying this principle to justify the jurisdiction of domestic regulations over cloud computing companies abroad would be unlikely. First, there has been fierce criticism over the passive personality principle since at least 1927.[187] In addition, applying a passive personality principle to domestic regulations on cloud computing companies could continue to cause uncertainty.

One commentator has argued for a possible application of the passive personality jurisdiction on cloud service providers.[188] Assuming a state criminalizes inadequate data protection by the service provider, an application of the passive personality principle might be applied in a scenario where it is difficult to determine exactly where the "harm" occurred, for instance, where there is a data transfer across multiple jurisdictions and third-party servers.[189] The state of incorporation may not have any incentive to bring actions against the provider, whereas the state of the national harm may have a desire to protect those abroad.[190] A serious problem arises, though, if all states seek to apply laws this way. The service provider would face high costs of uncertainty in determining which legal regimes it must conform to. Given how easy it is for a person to create a fake account and lie about their country of origin online, a provider might be subject to a

183. *See* CHERTOFF GROUP, *supra* note 60, at 5 (noting the current dominance of U.S.-based companies in the cloud computing industry).

184. *Id.*

185. *Id.*

186. Narayanan, *supra* note 5, at 799 (examining the application of the nationality principle).

187. *See* RYNGAERT, *supra* note 53, at 93.

188. *See* Narayanan, *supra* note 5, at 799 (stating that application of the passive personality principle would be beneficial given the difficult nature in tracking data in the cloud).

189. *Id.*

190. *Id.*

jurisdiction it did not expect to be under. If all states apply this principle, service providers might fear expanding beyond domestic borders, which would severely hinder the growth of the industry.

In the end, switching the focus on to the nationality of the user would be a big step forward in bringing laws like the SCA and RIPA into the twenty-first century. While there are still gray areas and several downsides in using this approach, it would hopefully lead to greater international cooperation and reinforce the notion of international sovereignty.

C. *Prong Two: Refining the MLAT Process*

In addition to redefining the jurisdictional terms of the SCA and its international analogues, the second part of a workable solution would be to reform the MLAT process between countries.[191] If the process was reformed, countries might have less of a desire to find ways to execute warrants for data on their own. Many decry the MLAT for being too cumbersome and time consuming; thus any reform would have to address the issue of expediency.[192] One group has suggested that a time limit be tied to the nature of the case at hand, so that routine matters are given more time while more pressing cases have an "express lane."[193] Such an express lane is needed, especially in today's world where cybercrimes are committed with increasing speed. Another author suggests that the MLAT process should create online submission forms for all agencies, instead of relying on paper and email.[194] Of course, this recommendation touches on another area of improvement for the MLAT process—the need for increased funding to gather more resources to deal with modern international crime.[195]

MLAT reform would also consist of some kind of reciprocity. As mentioned above, a downside to simply refocusing the territoriality principle is that it requires that states actually respect each other's sovereignty. A system that establishes some form of reciprocity would hopefully decrease the incentive for unilateral law enforcement actions. Of course, this would only work if both nations promised to exclusively use the MLAT system.[196] Therefore, another possible solution to further bolster the usefulness of the MLAT process is to require law enforcement agencies to use their best efforts to engage in the MLAT system before

---

191. *See* CHERTOFF GROUP, *supra* note 60, at 9.

192. *Id.* at 5.

193. *Id.* at 9.

194. *See* Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SECURITY J. (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age/ [https://perma.cc/BQ8D-NUDB] (archived Nov. 1, 2016).

195. *Id.*

196. CHERTOFF GROUP, *supra* note 60, at 9.

taking unilateral means to achieve their goals, otherwise known as a "first-use constraint."[197] Going hand in hand with a principle of reciprocity would go a long way in making the MLAT process an attractive alternative for law enforcement agencies.[198]

In theory, these reforms sound simple; however, putting them into practice is a harder task. Realistically, it is hard to expect law enforcement agencies to be able to deal with MLAT requests with the expediency always required. Therefore, some back door might be necessary to allow countries to bypass the MLAT process and use more unilateral measures in some circumstances.[199] Countries could include in the reformed treaties a term that limits the unilateral measures to "serious transnational crimes involving imminent threats of death."[200] The problem is that this creates the same back door that the SCA and RIPA already have. How would one define "a serious transnational crime" and "imminent"? Law enforcement wishing to forgo the MLAT process could overstate the severity of a crime in order to invoke this exigency provision.[201] This might mean that countries must consult each other about the case before letting such a provision be invoked. However, if the crime is indeed serious, there might not be time for such a consultation. These practical issues are one reason why even with MLAT reform, states may not fully embrace this solution.

Overall, it is clear that the MLAT process hinders rather than helps law enforcement. This deficiency has led to countries finding ways around it unilaterally at the expense of international comity.[202] The process must therefore be refined and made efficient so that law enforcement starts to think of the MLAT process first before using other routes. As a first step, the MLAT process should have increased funding and the warrant process should be streamlined.[203] Second, the MLAT system should provide for some form of reciprocity. A strong norm of reciprocity might encourage countries to resort to the MLAT process in the beginning of an investigation, instead of finding ways around it. However, being a norm, reciprocity might not be enough to encourage states to use the MLAT process if there is no enforcement mechanism to make sure the states do not cheat.

---

197. Hill, *supra* note 194.

198. *See, e.g.*, *id.* (noting the combined effects of a first use constraint and reciprocity approach).

199. CHERTOFF GROUP, *supra* note 60, at 9

200. *Id.*

201. *Id.*

202. *See* Hill, *supra* note 194 (highlighting how the current MLAT process forced the United States' hand).

203. *Id.*

V. CONCLUSION

At this moment in time, cloud computing is the way of the future.[204] However, its proliferation led to legal headaches, both domestically and internationally. Opposing laws and regulations already are a headache for companies that operate across borders. However, with the cloud, there is less clarity in determining the jurisdictional limits on countries' regulations. Thus, cloud computing service providers might potentially find themselves "in the unenviable position of choosing to comply with a U.S. court order or breaching EU laws."[205] This scenario, if left unchecked, could cut off the growth of the cloud industry, affecting not only businesses, but also the multitude of consumers who now use the cloud every day.

This Note has shown that the United States, applying the SCA, is not the only nation at fault. Countries like the United Kingdom have similar laws that allow law enforcement to access cloud data, without speaking on the issue of extraterritoriality. Thus, the only thing preventing other countries from also applying their laws extraterritorially is their domestic policies concerning the importance of international comity. A solution is needed that provides clarity to countries and corporations, increases international comity, and decreases diplomatic tensions, and is possible to attain. Relying on the traditional principles of jurisdiction, the best approach is for all countries to apply their laws concerning cloud computing with consideration of the nationality of the user. This would provide more certainty and lessen the fears of countries that their citizens are being spied on by other countries. However, to be realistic, the MLAT process must also be streamlined in order to encourage countries to use the MLAT process rather than attempt to unilaterally execute an extraterritorial warrant. While this two-step solution is not perfect by any means, and future technology may frustrate this approach, it is a good first step. What is not a good solution is for each country to continue acting alone, for this will leave everyone else in the dark and remove the benefits cloud computing offers in the form of global access to one's data.

*Matthew McKenna**

---

204. *See* Shane Paul Neil, *The New Space Race Is Happening a Lot Closer to Home*, HUFFINGTON POST (Mar. 1, 2016 2:37 PM), http://www.huffingtonpost.com/shane-paul-neil/the-new-space-race-is-hap_b_9353136.html [https://perma.cc/P9Y8-5BSW] (archived Nov. 1, 2016) (discussing how cloud computing technology is being utilized in cars and other gadgets).

205. Zoya Sheftalovich, *The Court Case that Could Sink Safe Harbor*, POLITICO (EUROPE EDITION) (Jan. 4, 2016, 11:22 AM), http://www.politico.eu/article/the-court-case-that-could-sink-safe-harbor-microsoft-department-of-justice-data-protection-ireland/ [https://perma.cc/33PA-H9S2] (examining the possible implications of the Second Circuit's decision in the Microsoft case).

* B.A. University of Florida; Candidate for Doctor of Jurisprudence, 2017, Vanderbilt Law School.