A U.S. Prosecutor's Access to Data Stored Abroad – Are There Limits?

Frederick T. Davis*

Summary

On September 9, 2015, the United States Court of Appeals for the Second Circuit heard argument on an appeal by Microsoft that raises an important, and relatively unexplored, question relating to the conduct of transnational investigations: can a U.S. prosecutor obtain data-based information stored outside the United States without recourse to an international agreement or convention, and without informing the country where the data are stored?[1] The appellate court may or may not address the international consequences of its decision, which were incompletely addressed by the parties. Because the issue will be a recurring one, it is useful to evaluate those consequences now.

The appeal is from an order by the District Court in the Southern District of New York compelling Microsoft to turn over to the United States Attorney e-mails and data relating to an unidentified customer of Microsoft (John Doe) who is the target of a criminal investigation. Microsoft resisted this order on the ground that John Doe had identified himself as a citizen of Ireland when he opened his account; that under its normal policy Microsoft keeps almost all data (including the content of any e-mails sent or received) of its customers on the server closest to the place of residence in order to minimize delays associated with "latency;" that the relevant data relating to John Doe were thus stored on a server in Ireland; and, that Microsoft disclaimed the legal obligation to obtain or produce data stored on its server in Ireland, although it had the technical ability to do so.[2] A magistrate judge ordered Microsoft to provide the information, and this decision was affirmed by a judge of the district court. Microsoft's appeal has been supported by an unusually large number of "friend of the court" briefs including from the Republic of Ireland, a Member

* Former Assistant United States Attorney, Southern District of New York; Member of the Paris and New York Bars. The author gratefully expresses his appreciation to Ryan Mullally, a third-year law student at New York University School of Law, for his contributions to this article.

1. For a useful description of the argument, at which the author of this article was also present, see Alex Ely, *Second Circuit Oral Argument in the Microsoft-Ireland Case: An Overview*, LawfareBlog (Sept. 10, 2015, 5:08 P.M.), www.lawfareblog.com/second-circuit-oral-argument-microsoft-ireland-case-overview?utm_source=dlvr.it&utm_medium=twitter. The panel reserved decision; a decision may issue at any time, but is not likely until late 2015 or sometime in 2016.

2. *In re* Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 15 F.Supp.3d 466, 468 (S.D.N.Y. 2014) [hereinafter Magistrate Judge's Opinion].

of Parliament of the European Union, a number of service providers (such as Apple, Verizon, Accenture, and many others), as well as constitutional law groups.[3]

This article will focus on a question that may or may not be addressed by the court of appeals, but which will inevitably have a significant bearing on how its decision may be received outside the United States: whether the district court's order complies with principles of international law, and in particular, with principles relating to the appropriate limits of a country's exercise of legislative, judicial, or police power when that exercise may have an impact on another country's interests. This is important because a decision widely understood as contravening international law—particularly if it is viewed as not respecting principles that other countries would respect if the issue were to arise there—could lead to negative consequences, such as decreased cooperation in transnational criminal matters, or retaliation against U.S. law enforcement authorities or service providers.

Because of this focus, there are a number of issues vigorously discussed in the parties' submissions and by the *amici curiae* that will not be addressed here, even though they are important and could be dispositive of the appeal. The two principal issues not addressed here are:

- *The proper interpretation of the Stored Communications Act (SCA).* The SCA was adopted by the U.S. Congress in the mid-1980s, before e-mail became the dominant and ubiquitous form of communication that it is today. Many of the arguments made to the magistrate judge and the district court concerned its proper interpretation. This article will assume that however the court of appeals decides issues under the SCA, its application to data stored in Ireland will be viewed by other countries as a question of "extraterritoriality."
- *The Constitution of the United States.* Some of the friends of the court urge that protections provided in the U.S. Constitution, notably the Fourth Amendment's limitations on official searches and seizures, bear on the court's analysis.[4] Again, this article offers no opinion on this question, but simply assumes that however the court deals with domestic constitutional issues, the result should also be analyzed from an international legal perspective.

This article also assumes the procedural regularity of the prosecutorial process—that is, that the prosecutor had a sufficient basis to seek the information held by Microsoft, and followed appropriate criminal procedures in doing so.

I. The Facts and Procedural History

The key facts and the procedural history of the Microsoft matter appear to be typical of a situation capable of frequent iteration. They are relatively simple.

As noted, John Doe is being investigated by the federal prosecutor in New York for possible violations of federal criminal laws. In the course of this investigation, the investi-

3. Microsoft Corp. Blogs, *Business, Media and Civil Society Speak Up in Key Privacy Case*, OFFICIAL MICROSOFT BLOG (Dec. 15, 2014), http://blogs.microsoft.com/blog/2014/12/15/business-media-civil-society-speak-key-privacy-case/.

4. *See, e.g.*, Brief for *Amici Curiae* Brennan Center for Justice at NYU School of Law, et al. in Support of Appellant, *Microsoft Corp. v. United States*, No. 14-2985-cv (filed Dec. 15, 2014), *available at* https://www.brennancenter.org/sites/default/files/legal-work/141215%20-%20BCJ%20Microsoft%20Ireland%20Amicus%20%28FILED%29.pdf.

gators learned that John Doe maintained a personal e-mail account with Microsoft. In search of evidence or leads relevant to the investigation, the prosecutor decided to obtain copies of John Doe's account information, including e-mails sent and received by him. Obtaining information from third parties about a person under investigation is, of course, a standard investigative procedure; requests to service providers for this purpose are made constantly.[5]

In the John Doe case, and pursuant to SCA procedures described in more detail below, the prosecutor applied to a federal judge for, and was granted, a warrant that directed Microsoft to produce to the prosecutor (without alerting John Doe) copies of all e-mails stored in his account, all information relating to his identity (such as the name and addresses provided), and any other information stored therein (such as names and addresses of correspondents).[6] As a frequent recipient of such official demands, Microsoft maintains a criminal compliance office tasked with responding to them; this office has the technical capacity to find and retrieve data maintained by its customers, even if the data are maintained outside the United States.[7] The compliance office determined that John Doe had identified himself as a resident of Ireland and that, consistent with standard Microsoft policy, as well as to minimize performance delays caused by latency in the event of increased distance between user and server,[8] John Doe's account was "hosted" on a server maintained by Microsoft in Dublin, Ireland.[9] As a result, all except a very small amount of the data sought by the government's warrant did not exist on any U.S. server, but could only be found in Ireland.[10] The small amount of data maintained in the U.S. consisted of information sufficient to identify the John Doe account and point to its location in Ireland, as well as a small amount of quality control information, but apparently did not contain any content of investigative use to the prosecutor.[11]

Upon learning of the location of the data, Microsoft informed the government that it would provide the (essentially useless) U.S.-based information, but would not provide information from its Irish server, even though it had the technical ability to obtain it by taking simple steps in the U.S. without apparent undue cost or difficulty.[12] Upon the refusal of the prosecutor to accept this, Microsoft filed a motion to quash the warrant on the basis that it was not authorized by the SCA and that it called for an extraterritorial application of U.S. laws, which was neither intended nor appropriate.[13] The magistrate

5. While agencies do not report the number of subpoenas they issue per year, the figure is thought to be huge. For example, *Wired* reported that AT&T responded to 131,400 subpoenas for customer information in the year 2011 alone. David Kravits, *We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena*, WIRED (Aug. 28, 2012, 6:00 AM), http://www.wired.com/2012/08/administrative-subpoenas.

6. *See* Magistrate Judge's Opinion, 15 F. Supp. 3d at 468.

7. *See id.* at 466, 468.

8. In this context, latency refers to the risk of slower responsiveness in the use of e-mail (or other internet functions) which may be caused by increased distance between user and server. *See* Margaret Rouse, *Latency*, WHATIS.COM, http://whatis.techtarget.com/definition/latency (last updated Nov. 2014).

9. *See* Magistrate Judge's Opinion, 15 F. Supp. 3d at 468.

10. *Id.*

11. *Id.*

12. *Id.*

13. *Id.* at 470.

judge denied this application in a twenty-six page written opinion. His decision was reviewed by a judge on the district court, who affirmed it.[14]

II. The Court's Decision

Much of the magistrate judge's opinion explored the SCA procedures for the prosecutor to obtain the John Doe data. The Court noted that the SCA was an attempt by the U.S. Congress to provide mechanisms to balance the largely opposing needs of, on one hand, governmental access to information in criminal and other contexts, and, on the other hand, the privacy rights of individuals.[15] Since the SCA was adopted at a time when data storage was in a relative infancy, it speaks in general terms and does not, for example, single out e-mails for specific treatment. It nonetheless provides a straightforward approach to the basic circumstance presented in the John Doe case by offering the prosecutor three different procedures to obtain personal information, each with a different burden of proof and judicial oversight depending on the intrusiveness of the inquiry.

The simplest procedure is for the prosecutor to issue an administrative subpoena, which the prosecutor can easily do in the name of the grand jury, in order to compel the information holder (such as Microsoft) to produce designated information.[16] The prosecutor can issue such a subpoena without any judicial intervention, and without any specific demonstration of need.[17] But under the SCA, the subpoena approach has some very important limitations:

- It permits the prosecutor to only obtain basic customer information, unopened e-mails more than 180 days old, and opened e-mails;[18] and
- The prosecutor must give notice to the customer, although notice may be delayed for up to ninety days upon the written certification of a supervisory official;[19]
- If the prosecutor delays giving notice, he or she may request a court order barring the internet service provider (ISP) from notifying the customer for a like period.[20]

The prosecutor can alternatively ask a judge to issue a court order, which permits access to further information in addition to that available under a subpoena, including a history of all e-mails sent or received by the customer (although not their content). The court order procedure differs from the issuance of a subpoena in certain respects:

- The prosecutor cannot issue it unilaterally, but must demonstrate to a judge "specific and articulable facts showing that there are reasonable grounds to believe" that the

14. *In re Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp.*, Nos. M9-150, 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014) (slip copy) [hereinafter District Court Opinion].

15. *See* Magistrate Judge's Opinion, 15 F. Supp. 3d at 470.

16. *Id.* at 468.

17. In the federal system, a recipient can challenge a subpoena on the ground that "compliance would be unreasonable or oppressive." FED. R. CRIM. P. 17(c)(2).

18. As noted, the SCA does not specifically mention "e-mails" as such, but rather talks about different varieties of "stored data." The application of the SCA to e-mails, and development of the distinctions noted here relating to age and status as "opened" or "unopened" resulted from judicial interpretation. *See* Magistrate Judge's Opinion, 15 F.Supp.3d at 469 n. 2. *See generally* O.S. Kerr, *A User's Guide to the Stored Communications Act, and a Legislator's Guide to Amending It*, 72 GEO. WASH. L. REV. 1208 (2004).

19. Kerr, *supra* note 18, at 1233.

20. *Id.*

information sought will be "relevant and material to an on-going criminal investigation";[21] and

- The prosecutor must provide notice to the affected party. Such notice cannot be delayed unilaterally, but can be delayed by court order and the judge can again bar the ISP from notifying the client/subscriber for a like period.[22]

Finally, the SCA permits the prosecutor to ask a judge to issue a warrant, which permits the prosecutor to obtain, in addition to information obtainable under a court order, unopened e-mails stored for less than 180 days, without informing the account holder.[23] Under the Federal Rules of Criminal Procedure, a judge can issue a warrant only upon the prosecutor showing probable cause of a belief that the information sought will provide evidence of a crime or the fruits thereof—a somewhat higher standard than the reasonable grounds necessary to obtain a court order.[24] Neither the SCA nor the Federal Rules require notice to the customer for the execution of such warrants.

None of the SCA provisions summarized here specifically addresses their intended extraterritorial reach—that is, whether they should or should not apply when responsive information is located outside the United States.

III. The Court's Reasoning

Microsoft's principal argument was appropriately described by the magistrate judge as "simple, perhaps deceptively so."[25] It argued that, under accepted jurisprudence, a warrant issued under Rule 41 of the Federal Rules of Criminal Procedure is limited to the territory of the United States and cannot be exercised outside of it; thus, the warrant issued here could not be executed upon data found in Ireland.[26] Magistrate Judge Francis rejected this argument.[27] His principal bases for doing so were two:

- First, he noted the traditional basis for restricting the execution of a warrant to U.S. territory. Historically, a warrant authorizes a law enforcement officer to enter a physical place (such as a home or place of business); thus, in that context, it would be clearly inappropriate for such an officer to do so outside the United States.[28] Here, he reasoned, no official act would take place outside the U.S. at all because the warrant called for Microsoft to obtain, and then produce, the requested information while staying in the United States.[29]
- Second, he noted that, historically, both subpoenas and court orders applicable to lesser intrusions, as noted above, were not limited to information located within the

21. *Id.*
22. *Id.* at 1234.
23. *Id.* at 1218.
24. The Sixth Circuit held that to the extent the SCA purports to allow the government warrantless access to e-mail content, it is unconstitutional. United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). The *Warshak* ruling has not been tested in the Supreme Court, which suggests that agencies have largely conformed to the decision and sought out SCA "warrants" rather than subpoenas or court orders.
25. Magistrate Judge's Opinion, 15 F.Supp.3d at 470.
26. *Id.*
27. *See id.*
28. *See id.* at 473.
29. *Id.* at 472.

United States.[30] It has long been the law, for example, that a person or corporation located in the U.S. must respond to a subpoena calling for information located outside the U.S. if it "controls" that information, i.e. is legally and physically able to access and produce it.[31] Reasoning that the warrant was in fact a "hybrid" structure, the Court concluded that there is no reason to believe that the Congress intended a broad extraterritorial reach for subpoenas and court orders, but a much more restricted one for warrants.[32]

In a short concluding section of its opinion entitled "Principles of Extraterritoriality", the magistrate judge reasoned that concerns relating to the application of U.S. laws outside the country's borders "are simply not present here."[33] He noted that the *Morrison*[34] and *Kiobel*[35] Supreme Court decisions created a strong presumption that U.S. legislation applies only within the country's borders, absent a showing of legislative intent otherwise, and implicitly acknowledged that nothing in the SCA specifically evidenced an intent that it should apply outside U.S. borders.[36] He nonetheless concluded that *Morrison* and *Kiobel* do not apply because Microsoft was located in the United States and would comply with the warrant without leaving the United States or committing any act outside of it: the warrant "places obligations only on the service provider [that is, Microsoft] to act within the United States."[37] The Court ended its discussion of extraterritoriality noting that: "[A]n SCA warrant does not criminalize conduct taking place in a foreign country; it does not involve the deployment of American law enforcement personnel abroad; it does not require even the physical presence of service provider employees at the location where data are stored."[38]

IV. Discussion

A. Extraterritoriality: Legal Limits on the Exercise of Sovereignty

The Microsoft appeal implicates classic principles of international law defining the limits of the territorial reach of a country's laws and their execution, and requires their application to relatively recent—and fundamentally disruptive—technological and commercial realities that did not exist when the prevailing rules relating to extraterritoriality were developed.[39] As will be discussed below, rules relating to sovereignty and its limits emerged from contexts implying a close and intuitively obvious link between the activity to be regulated and the actual place (or territory) involved.[40] When applied to data held in the "cloud" and frequently stored on servers physically located in locations distant from

30. *Id.* at 471-72.
31. *See, e.g.*, Marc Rich & Co., A.G. v. United States, 707 F.2d 663, 667 (2d Cir. 1983).
32. Magistrate Judge's Opinion, 15 F.Supp.3d at 471-72.
33. *Id.* at 475.
34. Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 255 (2010).
35. Kiobel v. Royal Dutch Petroleum Co., 133 S. Ct. 1659, 1664 (2013).
36. *See* Magistrate Judge's Opinion, 15 F.Supp.3d at 475-76.
37. *Id.* at 476.
38. *Id.* at 475.
39. This article addresses "international law" only in the context of the extraterritorial reach of a country's powers. International legal principles may also apply to the rights of individuals. That topic is not addressed in the present article.
40. *See* 2 M. Cherif Bassiouni, International Criminal Law 158 (3d ed. 2008) (footnote omitted).

activity that one country may wish to regulate, classic rules of international law may be difficult to apply, and may require sophisticated analysis of the principles at stake.

The limits of a state's right to project its laws or powers extraterritorially are sometimes viewed as having three components: the "power to prescribe," that is, the power to adopt laws affecting conduct; the "power to adjudicate," consisting of the power of a country's courts to issue valid decisions relating to the questions and persons before them; and the "power to execute," which refers to the power to enforce laws or judgments.[41] These powers belong to the sovereign, and traditionally have been limited to the sovereign's territory:

> The powers to prescribe, adjudicate, and enforce derive from sovereignty; thus, the exercise of national criminal jurisdiction has traditionally been linked, if not limited, to the territory of a state and, by extension, to the territory under the dominion and control of a given legal authority exercising de jure or de facto sovereign prerogatives.[42]

All three elements of sovereignty may be implicated when a prosecutor seeks information stored abroad: doing so implicates the power of Congress to apply provisions of the SCA (and of U.S. criminal laws generally) outside the territory of the U.S.; the adjudicatory power of U.S. courts (among other things, to issue warrants or court orders that may have impacts beyond U.S. borders); and the power of enforcement agencies to enforce the SCA, the warrants issued by US courts, and other mechanisms that may be involved in official pursuit of data stored outside the U.S.[43]

In a general but very important sense, all three limits on the exercise of sovereignty rest on two principal concepts: that application of one country's laws outside of its territory must be based on a reasonable and valid state interest; and, secondarily, that its interpretation and execution must take into account the reasonable and valid interests of other states. The jurisprudence developing these principles has developed from two principal conclusions:

- Every state is considered to have the power to address conduct that takes place on its *territory*, whether done by a citizen or not.[44]
- Every state is considered to have the power to address the conduct of its *citizens*, whether or not that conduct takes place on its territory.[45]

While simple in theory, both principles have evolved in ways that raise particular questions in the context of the Microsoft appeal.

The principle of territoriality has been expanded by the so-called "effects test." This approach expands the valid exercise of state power beyond addressing acts *committed* on its territory to include acts the effects of which (even if committed overseas) are *felt* on a state's territory.[46] The classic example of this analysis is a cartel where the participants

41. *Id.*; *see* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS OF LAW OF THE UNITED STATES § 401 (AM. LAW INST. 1987) (hereinafter "RESTATEMENT THIRD").

42. *See* 2 BASSIOUNI, *supra* note 40.

43. *See* RESTATEMENT THIRD §§ 401-02.

44. *See* S.S. Lotus (Turk v. Fr.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7), ¶ 45.

45. RESTATEMENT THIRD §§ 402, 421.

46. *See* 2 BASSIOUNI, *supra* note 40, at 160 (This is sometimes referred to as the principle of "objective territoriality" or "passive personality").

may enter into, and execute, an agreement to fix prices without ever setting foot in a country that nonetheless would suffer the economic consequences of an illegal agreement.[47] The effects test was developed in U.S. jurisprudence to investigate and prosecute overseas cartels, and was approached warily by countries in Europe;[48] more recently courts and administrative agencies in the European Union have generally adopted the concept.[49]

While external application of national laws on the basis of citizenship raise few questions when applied to natural persons, it becomes increasingly complicated when applied to corporations (and other synthetic "persons") because the citizenship (generally understood to be the place of incorporation or its principal place of business) of a company can be adjusted almost at whim by its owners through myriad means of incorporation of parents and subsidiaries, and other corporate relationships.

V. Technical & Commercial Developments That Affect the Analysis

Changes in technology over the last generation have, self-evidently, been vast; they will surely continue into the future. One general phenomenon bears emphasis here, which may be called the phenomenon of "deterritorialization" or "delocalization." Traditionally, laws and traditions protecting privacy have focused on principles linked to a physical place or *territory*. The Fourth Amendment to the United States Constitution, for example, refers to "the right of the people to be secure in their persons, houses, papers, and effects."[50] The reference in the same Amendment to the requirement of a "warrant" as a prerequisite to seizing a person or thing, and the insistence that it not be issued other than upon "probable cause," had a clear territorial, or physical, reference: whether to detain a "person," enter a "home," or seize a "paper" or "effect"—all required physical access to a specific place.[51] It is thus clear why, traditionally, and as set forth in Rule 41 of the Federal Rules of Criminal Procedure, a warrant could not have any effectiveness outside of the territory of the United States—precisely because a warrant contemplated that a state actor (such as the police) would act in a physical place (the location of a person or a thing), it seems obvious that its execution could not occur outside of the territory of the United States without infringing on the sovereign rights of another country.[52] As one oft-quoted

47. U.S. v. Aluminum Co. of America, 148 F.2d 416, 443 (2d. Cir. 1945) (considered to be the first example in US law of the modern effects test). For a discussion of the effects test under US law see Kathleen Hixson, *Extra Territorial Jurisdiction Under the Third Restatement of Foreign Relations Law of the United States*, 12 FORDHAM INT'L L.J. 127 (1988).

48. Hixson, *supra* note 47, at 139-140.

49. See Kenneth S. Gallant, *Jurisdiction to Adjudicate and Jurisdiction to Prescribe in International Criminal Courts*, 48 VILL. L. REV. 763, n.214 (2003), for a list of cases in multiple nations around the world where versions of the "effects test" have been applied. For a discussion of the effects test under the law of the European Union, see Laurent Cohen-Tanugi, *The Extraterritorial Application of American Law: Myths and Realities*, EN TEMPS RÉEL 1, 11-14 (2014), https://lct2013.files.wordpress.com/2013/09/extraterritoriality-paper-anglais-final.pdf.

50. U.S. CONST. amend. IV.

51. *Id.*

52. In, *In re Terrorist Bombings of U.S. Embassies in E. Africa*, 552 F.3d 157, 169 (2d Cir. 2008), the Second Circuit noted that "seven justices of the Supreme Court in *United States v. Verdugo-Urquidez*, 494 U.S. 259, 278 (1990) endorsed the view that U.S. courts are not empowered to issue warrants for foreign searches." *Magistrate Judge's Opinion*, 15 F. Supp. 3d at 476 (further holding that such limitations only apply to conven-

opinion put it, one state "may not exercise its powers in any form in the territory of another state."[53]

In the eighteenth century and well into the twentieth, information was stored in "papers," very much linked to the "place" where papers were stored. The early phases of the computer revolution and the storage of information as digitized data did not cause a huge change in this traditional frame of reference, because data were initially stored on fixed media such as floppy disks and hard drives; those media—much like "papers"—had a physical location, and it did not cause too much difficulty to adapt Fourth Amendment jurisprudence, and rules relating to searches and seizures, to them.[54] Furthermore, as a practical matter people (including suspected criminals) tended to store information in a physically—and thus local—accessible place, and could generally not hide incriminating information abroad.[55]

The explosion of cheap and high-speed data transmission together with radically reduced costs of storage changes this. As one writer recently observed, "the infrastructure of the internet means that data are not territorially bound."[56] While people continue to store data on local hard drives and memory sticks, data are increasingly stored at the very least on a "network" of linked computers and often in "the Cloud."[57] The Cloud, in turn, may consist of any number of different phenomena, sometimes in tandem, including the following:

- Data may be stored on a server that is extremely remote from the persons storing (and later getting access to) the data; this may include storage in a completely different country.[58]
- Casual users of the Cloud may not know or care where their data are stored, but someone seeking anonymity can deliberately choose a remote location where third-party access is restricted or protected by local law or custom.[59]
- Due to the low cost of data storage and the need for security, there are often automatic backups so that the same data appear simultaneously in more than one place.[60]

---

tional warrants, not SCA hybrid warrants which do not interfere with foreign territory the same way); *see also* FED. R. CRIM. P. 41.

53. *S.S. Lotus* 1927 P.C.I.J. (ser. A) No. 10, ¶ 45.

54. U.S. CONST. amend. IV.

55. *Id.*

56. DAVID ANDERSON, A QUESTION OF TRUST: REPORT OF THE INVESTIGATORY POWERS REVIEW 51 (June 11, 2015), *available at* https://www.gov.uk/government/publications/a-question-of-trust-report-of-the-investigatory-powers-review.

57. *Id.*

58. Mathieu Gorge, *The Implications for Storage of EU Data Protection Regulation*, COMPUTER WKLY. (Aug. 2012), http://www.computerweekly.com/feature/The-implications-for-storage-of-EU-data-protection-regulation.

59. *See id.*

60. Paper and other traditional forms of information storage can, of course, be copied. The differences between paper and data copying are primarily two: a copy of data is remarkably cheap to make, store, and retrieve; and, while a "copy" of a physical document is almost always different in some way from the "original," generally speaking there is no such distinction between the "original" and the "copy" of digitized information—they are literally identical.

- At least with respect to data in transit, a "document" or other piece of information may be broken into "packets" of data and routed separately to a destination where they are reassembled.[61]
- While encrypting physical documents is difficult and expensive, encrypting digitized data is not.[62]

Still, further disassociation of data from territory may be possible. Some data storage companies have already spoken of creating "data farms" on the high seas where, at least in theory, the physical location of the data is not subject to any country's jurisdiction;[63] it is even possible to imagine storing data on satellites in space.

Separately, technology offers a different threat to law enforcement authorities if data storage companies adopt and make available to their customers the fruits of so-called "public-key cryptography" technology: Data companies could easily advertise that their customers can choose an encryption system where the "key" to reopen encrypted communications is retained by the customer alone.[64] Under this scenario, an ISP confronted with a warrant could hand over encrypted data, but neither the ISP nor the investigator could decrypt it.[65] This would permit encryption that, under current technology, cannot be broken (or at least cannot be broken without an undue expenditure of time or resources), and thus access by a State to information stored by a customer could not be had from the storage provider at all, irrespective of the legal procedure followed or the demonstration of need.

The "delocalization" of data may have limits as countries try to protect data stored in them by laws inhibiting use of the Cloud or other technologies that contribute to delocalization. Whether or not such laws increase and are effective, is open to question;[66] and, in any event, as a practical and commercial matter, remote Cloud storage appears to be increasing rapidly.[67]

Analysis of international law principles depends in part on weighing the respective interests of participants to determine whether there is any true conflict between the legally protected interests of different countries, and to weigh them. The participants whose interests apply to the Microsoft case are the "Requesting Country", the United States, acting through the federal prosecutor); the "Host Country", Ireland, where the relevant data are stored; the "Owner" of the data, John Doe; and the "Internet Service Provider" (ISP), Microsoft.[68]

---

61. Anderson *supra* note 56, at 51.

62. Vivek Mohan & John Villasenor, *Decrypting the Fifth Amendment: The Limits of Self-Incrimination in the Digital Era*, 15 U. PA. J. CONST. L. 11, 22 (2011).

63. *Magistrate Judge's Opinion*, 15 F.Supp. 3d at 475 (*citing* Steven R. Swanson, *Google Sets Sail: Ocean–Based Server Farms and International Law*, 43 U. CONN. L. REV. 709, 716–18 (2011)).

64. Glenn Fleishman, *How to Keep Your Email Private with PGP Encryption on Your Mac*, MACWORLD (Mar. 2, 2015), http://www.macworld.com/article/2890537/how-to-keep-your-email-private-with-pgp-encryption-on-your-mac.html (last visited Oct. 5, 2015) (a guide for new users of public-key cryptography tools).

65. *See id.*

66. *See* Daniel Castro, *The False Promise of Data Nationalism*, INFO. TECH. & INNOVATION FOUND. (Dec. 9, 2013), http://www.itif.org/publications/2013/12/09/false-promise-data-nationalism.

67. *See id.*

68. *Magistrate Judge's Opinion*, 15 F. Supp. 3d at 468.

A. The Requesting Country

The obvious and legitimate interest of the prosecutor is to obtain information in aid of his or her investigation.[69] It is essentially irrelevant to the prosecutor where that information is stored. Thus, the interest of the prosecutor is no less and no more legitimate with respect to data stored overseas than with respect to information traditionally obtained through "search and seizure" procedures domestically. The United States does have a secondary interest in maintaining good diplomatic relations with other countries, from which it may seek cooperative help in criminal investigations, and thus in observing international rules, since rejecting them may diminish cooperation.

B. The Interest of the Host Country

The interest of the host country is perhaps the most important to evaluate, because it touches on principles of sovereignty and will likely be an important factor in the legal, economic, or diplomatic reactions that a decision might cause.

While Ireland submitted a brief as *amicus curiae* in the Microsoft appeal, it did not specifically take a position on how the Court of Appeals should rule; nor did it explicitly state its interest in the matter.[70] Its principal purpose was to express its willingness to fulfill all its obligations under its Mutual Legal Assistance Treaty with the U.S., and to bring to the Court's attention a recent decision of the Supreme Court of Ireland relating to access to bank data held abroad.[71] Evaluating the inherent interests of any country hosting data that may be sought by US procedures is nonetheless critical to a reasoned analysis.

The record is incomplete with respect to two issues of possible relevance.[72] First, it is unclear the extent to which John Doe is, in fact, a citizen or resident of Ireland. While he indicated on an application for a Microsoft account that he resided there, this was not verified.[73] Second, and more broadly, it is unclear whether John Doe's activities under investigation had any link to Irish territory, apart from the claimed residence of the owner and the fact that Microsoft chose to store his e-mail data there.[74]

Depending on these two variables, one could construct hypothetical situations where the host country's interests could be quite different:

- It is possible that Mr. Doe is not only an Irish citizen, but that all of his activities relevant to the U.S. investigation took place in Ireland; or, alternatively
- It is also possible that he is a U.S. and not an Irish citizen; that he has never even been in Ireland; that all his potentially criminal acts (including e-mail correspondence) took place in the United States; and, that his e-mail data are stored in Ireland only because he lied in providing account opening information to Microsoft.

---

69. *Id.*

70. *See* Brief for Amicus Curiae Ireland, at 3, *Magistrate Judge's Opinion*, 15 F.Supp.3d 466 (S.D.N.Y. 2014) (No. 14-2985) (filed Dec. 8, 2014), *available at* http://digitalconstitution.com/wp-content/uploads/2014/12/Ireland-Amicus-Brief.pdf.

71. *Id.*

72. *Magistrate Judge's Opinion*, 15 F. Supp. 3d at 475.

73. *Id.*

74. *Id.*

- Mr. Doe also could have been an Irish participant in a criminal gang or enterprise located principally in the U.S.: without leaving Ireland; he could have worked with co-conspirators operating in the U.S. by (for example) receiving the financial fruits of their crime and laundering it in Ireland.

In the first and third hypotheticals, Ireland might claim a genuine interest in protecting the privacy of one of its citizens. In the second, it is more difficult to determine Ireland's real interest in the John Doe case specifically, but it may have more general concern about U.S. access to data stored in Ireland.

Viewed generally, a host country may have interests in data stored within its territory, irrespective of the question of citizenship or territory-based activity:

- First, a host country may have an economic interest in encouraging "data farms" on its territory, which could be expected to bring some revenue, and would worry that its reputation for such activities would be adversely affected by perceptions that data stored there can be accessed from outside the country.[75]
- Second, and much more importantly, it will certainly have a general, but important, concern about its "sovereignty," and may well take offense to a ruling by a U.S. court that any company that stores its data in Ireland can be forced to turn over that data to U.S. prosecutors without going through formal diplomatic channels, and thus that data stored in Ireland can be produced overseas without Ireland even knowing.[76]

The terms of some mutual legal assistance treaties and legislation relating to international data transfer provide insight into the sovereign interest of a country in data stored on its territory:

- A number of countries have adopted so-called "blocking statutes," the purpose of which is to prohibit the transfer of information outside of the country without going through international conventions or agreements that, at a minimum, provide authorities in the host country with notice of any request for information and the opportunity to exercise control over the release of such data outside of its territory.[77] Under the Court's existing ruling in the Microsoft case, no host country would even have a right to be informed if a company storing data on their territory were obligated to turn such data over to a U.S. prosecutor, thus eviscerating the effect of national legislation such as the "blocking" statutes.[78]
- A number of international treaties clearly contemplate some degree of supervision or control by a host country over access to data stored there. For example, Article 9(2)(a) of the Agreement on Mutual Legal Assistance Between the European Union and the United States of America, signed in 2003, provides that the host country (or, as used in the Agreement, the "requested country") to whom a request for mutual assistance is made may add certain "limitations" on information transferred "to pro-

75. *Id.*

76. *See id.*

77. For example, France's so-called "Blocking Statute" makes it a crime to transfer certain kinds of information outside of France for use in an "administrative or judicial proceeding" other than pursuant to international agreements or conventions. *See* Grosdidier, *The French Blocking Statute, the Hague Evidence Convention, and the Case Law: Lessons for French Parties Responding to American Discovery*, 50 TEX. INT'L L.J.F. 11 (2014).

78. *Id.*

tect personal and other data."[79] An "explanatory note" to this Article makes it clear that the host country must be in a position to make a case-by-case determination of the need for such protection in order to avoid an overbroad or inflexible rule.[80]

Article 9(2)(b) is meant to ensure that refusal of assistance on data protection grounds may be invoked only in exceptional cases.[81] Such a situation could arise if, upon balancing the important interests involved in the particular case (on the one hand, public interests, including the sound administration of justice and, on the other hand, privacy interests) furnishing the specific data sought by the requesting State would raise difficulties so fundamental as to be considered by the requested State to fall within the essential interests grounds for refusal. A broad, categorical, or systematic application of data protection principles by the requested State to refuse cooperation is therefore precluded. Thus, the fact the requesting and requested States have different systems of protecting the privacy of data (such as, that the requesting State does not have the equivalent of a specialized data protection authority) or have different means of protecting personal data (such as, that the requesting State uses means other than the process of deletion to protect the privacy or the accuracy of the personal data received by law enforcement authorities), may, as such, not be imposed as additional conditions under Article 9(2)(a).[82]

This provision—found in an important treaty between the US and Europe relating to mutual legal assistance in criminal matters—clearly shows that both the United States and the countries in the European Union think that they have a say about whether to allow the transfer of data out of their respective countries. This interest would be thoroughly undermined by the current ruling in the Microsoft case, since it would permit the transfer of data out of Ireland without Ireland even being aware of the request or the transfer.

C. The Owner

John Doe may have two distinct and different interests: he has a personal privacy interest in resisting disclosure of his personal information, but he also has an interest in procedural regularity with respect to a criminal investigation of him.

From all that appears in the record, it seems that John Doe has no basis under U.S. law to contest the adequacy of the procedures used to obtain his information: Under the SCA and Rule 41 of the Federal Rules of Criminal Procedure, the prosecutor must have demonstrated to the satisfaction of a neutral judge that there was "probable cause" to conclude that John Doe was responsible for a federal crime, and that evidence in his e-mail account would shed light on this.[83] The public record does not disclose what that showing of probable cause was; for present purposes, the only appropriate presumption is one of regularity, that is, that a sufficient showing was made. While that showing was not one to which John Doe had the opportunity to oppose, under U.S. procedures he would

79. Agreement on Mutual Legal Assistance Between the United States of America and the European Union, E.U.-U.S., art. 9(2)(a), June 25, 2003, T.I.A.S. No. 10-201.1 [hereinafter Agreement on Mutual Legal Assistance].

80. Explanatory Note on the Agreement on Mutual Legal Assistance Between the United States of America and the European Union, E.U.-U.S., 3, June 25, 2003, T.I.A.S. No. 10-201.1.

81. Agreement on Mutual Legal Assistance, *supra* note 79, art. 9(2)(b).

82. *Id.*, art. 9(2)(a)

83. *See* Fed. R. Crim. P. 41.

get that opportunity if he is indicted and the fruits of an e-mail search were offered against him. On the present record, it is difficult to see how Mr. Doe could argue that Irish rather than U.S. standards should be used to evaluate whether he has been treated fairly. If John Doe was a legitimate target of a US criminal prosecution—that is, if the U.S. was "competent" to proceed against him—he would have no basis to argue that because of his Irish citizenship, or other non-U.S. contacts, he was protected by non-U.S. rules. Otherwise put, there is no international principle that suggests that prosecutors have to follow different rules when the target of their investigation is not a U.S. citizen.[84]

Under U.S. law, John Doe would not appear to have a separately enforceable means of protecting his privacy interests, other than by means of seeking suppression of the fruits of illegally obtained information in the event he is prosecuted. To the extent that he may have privacy rights under Irish law, his interests would thus merge with those of Ireland, which would enforce those laws.

D. The Internet Service Provider

The real interest of the ISP, in this case Microsoft, appears to be primarily commercial.[85] While Microsoft has vigorously pursued this appeal emphasizing the procedural restraints on governmental authority necessary to protect the privacy rights of its customers[86]—a theme also emphasized in the many amicus briefs filed by other commercial enterprises—the only basis for a non-vicarious (or non-altruistic) interest is the perceived risk of a competitive disadvantage if it is ordered to turn over John Doe's Irish data.[87] As the trial judge noted in his opinion, Microsoft is a large American company with the acknowledged technical ability to easily obtain the data that it elects to store overseas.[88] Microsoft (and similarly situated U.S. companies that appear as *amici*) are clearly concerned that an adverse ruling will be interpreted by potential customers to mean their data are not safe with an American service provider who can easily be forced to share data with the prosecutor, irrespective of the location of those data;[89] U.S. companies, in fact, appear

84. A non-citizen may have certain rights under diplomatic conventions applicable to the country where he is arrested, but that would not affect such a non-citizen's rights during an investigative phase.

85. *See* Brief for Appellant, *Magistrate Judge's Opinion*, 15 F.Supp.3d 466 (S.D.N.Y. 2014) (No. 14-2985) (filed Dec. 8, 2014), *available at* https://www.eff.org/files/2014/12/12/microsoft_opening_brief.pdf.

86. Microsoft's standing may be questioned. On July 21, 2015, the Appellate Division, First Department, of the Supreme Court of the State of New York ruled on an application by Facebook seeking an order that it should not have to respond to 381 "search warrants" served on it by the District Attorney seeking customer information, arguing a variety of privacy-related and overbreadth issues. The District Attorney challenged Facebook's "standing" to contest the application for the warrants. Without using the word "standing", the Appellate Division dismissed Facebook's appeal, noting that the real privacy interests were those of Facebook's customers, and that those interests were sufficiently addressed by the ability of the customers to seek suppression at trial of any fruits of improperly issued warrants. The case did not involve any international or extraterritorial issues. Microsoft joined a brief filed as *amicus curiae* supporting Facebook. *In re* 381 Search Warrants Directed to Facebook, Inc. v. N.Y. Cty. Dist. Attorney's Offfice, 132 A.D.3d 11, 14 N.Y.S.3d 23 (N.Y. App. Div. 2015).

87. *See*, *e.g.*, Brief for AT&T Corp. et al. as Amici Curiae Supporting Appellant at 2, *Magistrate Judge's Opinion*, 15 F.Supp.3d 466 (S.D.N.Y. 2014) (No. 14-2985), *available at* https://www.eff.org/files/2014/12/15/att_microsoft_ireland_amicus_brief.pdf.

88. *Magistrate Judge's Opinion*, 15 F.Supp.3d 467, 468 (S.D.N.Y. 2014).

89. *See* Brief for Appellant, *supra* note 85, at 17; *see*, *e.g.*, Brief for AT&T Corp. et al. as Amici Curiae Supporting Appellant, *supra* note 87.

to suffer from a lack of trust from clients and potential clients, especially since the disclosures made by Edward Snowden in June 2013 revealed the extent to which U.S. ISPs are forced to share data with national agencies.[90] A broadly worded adverse ruling could also damage their business by leading to scenarios where a U.S. court might hold them in contempt if they do not produce the requested data, when, at the same time, production of such data would be a punishable offence in the nation where the data are hosted.

VI. The Parties' Legal Positions

The outcomes proposed by the federal prosecutor and by Microsoft could not be more diametrically opposed.

A. The Position of the U.S. Government

The prosecutor argues that the issue is very simple because the courts have already ruled that any entity that is "present" in the United States (or that is subject to its personal jurisdiction) can be ordered to produce any data that it "controls," irrespective of the location of those data.[91] This position was essentially adopted by the District Court.[92] It raises a few questions:

While much of the discussion about the case has focused on the obvious fact that Microsoft is a large, and indeed iconic, American enterprise, the government's position, if adopted, would not be limited to U.S. companies. Rather, it would apply to *any* company over which the prosecutor can convince a court that it has power to enter a binding and enforceable order—that is, as to which the courts can exercise the "power to adjudicate."[93] While the breadth of this ruling might assuage somewhat of a concern that American companies would be singled out and thus suffer a competitive disadvantage, it may be difficult for non-U.S. companies to determine whether their activities in the United States in fact subject them to American personal jurisdiction, and some may be legitimately surprised by the exercise of U.S. "long arm" jurisdiction over them. It is, in fact, often difficult to determine the extent to which courts may exercise "personal jurisdiction" over parties based upon their activity on the internet.[94] Concerns about vulnerability to U.S. demands for data stored outside the United States may well convince non-U.S. ISPs not to compete in the United States by offering services there, or otherwise maintaining a "presence" in the United States.

The position of the United States government is particularly troublesome because it fails to recognize any legitimate interest at all in the countries where the data it seeks may be found. In taking this position, the prosecutor echoes the conclusion of the District

90. Mary Madden, Public Perceptions of Privacy & Security in the Post-Snowden Era, Pew Res. Ctr. 3 (2014), *available at* http://www.pewinternet.org/files/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf.

91. Brief for Appellee at 8, *Magistrate Judge's Opinion*, 15 F.Supp.3d 466 (S.D.N.Y. 2014) (No. 14-2985) (filed Mar. 9, 2015).

92. *Magistrate Judge's Opinion*, 15 F.Supp.3d at 474.

93. Brief for Appellee, *supra* note 91.

94. *See*, *e.g.*, Pierre Grosdidier, *When Internet Libel Lands You in an Out-of-State Court*, Law360 (Apr. 24, 2015, 10:33 AM), http://www.law360.com/articles/647249/when-internet-libel-lands-you-in-an-out-of-state-court.

Court, quoted above, that the Court's order does not raise "extraterritorial concerns" because it does not compel any activity to take place on foreign soil.[95] This reasoning, however, does not take into account the *effects* of the Court's order, which definitely would be felt on foreign soil to the extent that data found exclusively on it are produced in the United States, because it would deprive the host country of the ability to make a determination[96]—expressly permitted by the U.S./E.U. Treaty, for example[97]—whether a requested transfer violated its privacy or other laws. As noted, a purely "territorial" analysis has already evolved to consider the interest of the country where the effects are felt, and not just those where the acts took place.[98] While invoked as a basis to justify expanded U.S. authority to rule on activity taking place outside of the territory of the United States, it would logically imply that an appropriate exercise of that authority should consider the effects of U.S.-based activity that are felt elsewhere.[99] In a different context, when high tech criminals located outside the United States target U.S. victims by "hacking" or other means, they do so without in any way taking acts inside the United States; but, it is intuitively obvious that their acts implicate U.S. sovereignty (and thus the right of the U.S. to regulate or prosecute) because the "effects" of their acts are recognized there. It would thus appear logical that U.S. jurisprudence should consider the "effects" of its decisions outside the U.S.

B. The Position of Microsoft

Microsoft's position, supported by many amici curiae, is that the only means by which a United States prosecutor should be able to obtain data stored abroad is through an international treaty, bilateral agreement, or other state-to-state mechanism.[100] In so arguing, Microsoft appears to take for granted the interest of the host country. The rule it proposes, however, is both overbroad and inflexible and thus treats in the same way situations that may be quite different. One could imagine a situation involving the following hypothetical elements:

- An individual, we will name James Doe, is a U.S. citizen who is part of an organized U.S.-based criminal gang. Aware that e-mails, while useful to his nefarious plans, may be recovered through investigative means, James selects a non-U.S. ISP known to be based in, and to store its data in, the territory of a country that has no MLAT or similar agreement with the United States, and with which the United States has bad diplomatic relations. In filling out his account opening form, Mr. Doe lies and says that he is a citizen of the country hosting the service.
- Without once leaving the United States, Mr. Doe constantly uses his e-mail to reach out to fellow gang members, and also uses it to defraud victims—in short, his e-mail use in the United States generates very compelling proof of his crimes. But he carefully "wipes" his computers, so that the only place where the content of these communications can be found is on the server in the hostile country.

95. *Magistrate Judge's Opinion*, 15 F.Supp.3d at 475.
96. *See* Brief for Appellant, *supra* note 85, at 59.
97. Agreement on Mutual Legal Assistance, *supra* note 79, art. 13.
98. Gallant, *supra* note 49.
99. Brief for Appellee, *supra* note 91, at 26.
100. *See* Brief for Appellant, *supra* note 85, at 12, 49, 58.

Under Microsoft's analysis, it would appear that the prosecutor would be almost powerless to obtain these data, and would be reduced to applying diplomatic pressure to negotiate with the hostile foreign state.[101]

VII. An Approach that Conforms with International Legal Principles

A. The Scope of the Court's Review

A threshold issue (raised by the judges during oral argument, see *supra* note 1) is to identify the Court's role in interpreting the SCA and the criminal procedures followed here.

The prosecutor posits that the law in this area is settled, and that the Court should simply apply it. He relies in large part on two well-known principles.

First, he notes the following observation by the Court of Appeals nearly fifty years ago:

> It is no longer open to doubt that a federal court has the power to require the production of documents located in foreign countries if the court has *in personam* jurisdiction of the person in possession or control of the material.[102]

And second, he notes that the same court has often emphasized that "[t]he test for the production of documents is control, not location."[103]

This and similar precedent, in fact, would seem to support the prosecutor's position that when a judicial order is enforceable on a corporation or person acting in the United States, and is not an authorization to an officer to act outside of it (as with a traditional "warrant"), the issuing court need not consider the interests of the country where the data are stored. There are several reasons, however, why the Court should pause before mechanically applying this precedent.

First, virtually all of the "worldwide subpoena" cases such as *Marc Rich* involve bank or other commercial data.[104] Extending *Marc Rich* precedent to searches for private e-mails risks precisely the sort of intrusion into personal privacy that is a matter of intense international sensitivity, and that is the basis of international agreements protecting such interests, including those that address international requests for mutual aid in criminal investigations as noted above.[105]

Second, the *Morrison* and *Kiobel* decisions in the Supreme Court reflect a real seachange in the role of the courts in interpreting legislative mandates that touch on non-US interests. In each case, the Court revisited what it repeatedly called "judge-made rules," which were prior—often very well settled—decisions permitting extraterritorial application of legislation that was itself silent on whether it should apply outside of the United States.[106] The unambiguous message of the two decisions is that such precedent will be reviewed to scrutinize whether they reflected an actual and expressed legislative intent. As the *Kiobel* court emphasized:

---

101. *See id.* at 17.
102. U.S. v. First Nat. City Bank, 396 F.2d 897, 900-01 (2d Cir. 1968).
103. *Id.* (quoting *In re* Marc Rich & Co., 707 F.2d 663, 667 (2d Cir. 1983)).
104. *See, e.g.*, *In re Marc Rich & Co.*, 707 F.2d 663.
105. *See id.*
106. *See generally Morrison*, 561 U.S. 247; *see also Kiobel*, 133 S.Ct. 1659.

> For us to run interference in . . . a delicate field of international relations there must be present the affirmative intention of the Congress clearly expressed. It alone has the facilities necessary to make fairly such an important policy decision where the possibilities of international discord are so evident and retaliative action so certain. The presumption against extraterritorial application helps ensure that the Judiciary does not erroneously adopt an interpretation of U.S. law that carries foreign policy consequences not clearly intended by the political branches.[107]

On this basis, the Court concluded bluntly: "When a statute gives no clear indication of an extraterritorial application, it has none."[108]

It bears emphasis that not only the SCA but all of the legislative acts discussed in the decisions upon which the Prosecutor relies, including *Marc Rich* and its progeny, were silent on the question of their extra-territorial application.[109] The decisions permitting a "worldwide subpoena" do not reflect expressed legislative intent, but are precisely the sort of "judge-made rules" that the opinions in *Morrison* and *Kiobel* felt constrained to revisit. In *Morrison*, the Supreme Court did not hesitate to overturn nearly a half century of settled law in the Second Circuit regarding the extraterritorial reach of the federal securities law.[110] The appeals court here should assume that the Supreme Court may similarly review the "judge-made rules" upon which the prosecutor relies.

And finally, of course, virtually all of the cited precedent and legislation—indeed the very structure of the relevant discussion from which the precedent and legislation emerge—were based on frames of reference that have all but disappeared because of technological change. The very notion of the "location" of data, and the link between such location and all-important principles, such as personal privacy and national sovereignty, has fundamentally changed. As the panel noted during oral argument, these profound changes call for congressional action, but in the meantime, the courts must deal with them.[111]

B. A Nuanced Approach

Any ruling by the Court of Appeals will risk mischief if it attempts a simple "one rule fits all" rule, including either of those proposed by the parties. While there is an obvious need for administrative simplicity, the following procedures would not overburden the wheels of justice; they are far more likely to yield results that would be viewed outside the United States as consistent with international law—and thus would not cause an undue risk of retaliation.

If a prosecutor or other governmental authority seeks information stored as data, it can proceed using any of the SCA procedures according to the circumstances. An ISP receiving a subpoena, court order or warrant may resist compliance on the grounds that the data sought are located exclusively outside the United States only upon a showing that:

---

107. *Kiobel*, 133 S.Ct. at 1664 (internal quotations omitted).
108. *Morrison*, 561 U.S. at 255.
109. *See, e.g., In re Marc Rich & Co.*, 707 F.2d 663.
110. *See Morrison*, 561 U.S. at 255.
111. Ely, *supra* note 1.

1) There is an objective basis to believe that the Host Country may have an actual and valid interest in the data stored there, which may entail a showing that (a) the account holder is a verified citizen or resident of that country, *and/or* (b) the use of the account has been predominantly in the host country; *and*,
2) The host country in question has a demonstrably acceptable record working cooperatively with the United States through MLATs, international treaties, or other arrangements.

The prosecutor can rebut this by showing that:

1) There is objective basis to believe that the account holder actively used the account as part of a criminal act and while in the territory of the United States; *or*
2) There is an objective basis to believe that, while outside the United States, the account holder actively used the account as part of a criminal act that was intended to, and foreseeably will, have a material effect in the United States; *or*
3) The host country in fact is not cooperating effectively with the United States; *or*
4) There is a special emergency where recourse to bilateral cooperation would be ineffective.

Overlapping territorial jurisdictions, or "concurrent jurisdiction," is not a new concept. The paradigm example from the infamous *S.S. Lotus* case of two ships, flying the flags of different nations and colliding in international waters, shows that such occurrences were possible even without modern data processing and storage techniques.[112] In that case, both France and Turkey had territorial jurisdiction over their own ships, as extensions of their respective territories, so either country could have adjudicated the dispute.[113] In today's context, just because the United States may assert territorial jurisdiction over an ISP within its territory should not deprive Ireland or any country where data are found of the power to regulate or protect data found on their servers. But where ship collisions were a relatively rare occurrence, modern data storage techniques will frequently implicate concurrent jurisdiction as companies make use of remote data processing sites.

A legal framework that accounts for modern data storage practices must do more than inquire into whether a state has the power to compel data disclosure. And finding common ground requires a nuanced understanding of how the core issues may be viewed elsewhere. As the Microsoft case shows, U.S. analysis tends to focus on the police powers relating to the place where data are stored; a European analysis is likely to focus on the rights of the individual whose data are involved.[114] Any successful long term solution must meet the requirements of comity by balancing the legitimate interests of the countries that may be affected by the exercise of that power.

A very recent decision of the European Union's highest court, the European Court of Justice (ECJ), while not directly applicable to the Microsoft case, reflects very different

112. *S.S. Lotus*, 1927 P.C.I.J. (ser. A) No. 10.

113. *Id.* at 30-31.

114. For example, in June 2015, the French database protection agency known as the CNIL (*Commission Nationale de l'Informatique et des Libertés*) announced that in order to protect the "right to be forgotten" as that right is viewed in France, Google must eliminate links relating to complaining French citizens—even on servers located in, and primarily accessed from, the United States. *See* JEREMY FEIGELSON ET AL., DEBEVOISE & PLIMPTON, LLP, A NEW RULING BY THE FRENCH DATA PROTECTION AUTHORITY: IS THE RIGHT TO BE FORGOTTEN CROSSING THE ATLANTIC TO THE U.S.? (2015), http://www.debevoise.com/~/media/files/insights/publications/2015/06/20150624a_french_data_protection.pdf.

appreciations of data sovereignty between the United States and Europe, the sensitivity of relations on those issues, and the economic and diplomatic interests at stake. In a landmark decision handed down on October 6, 2015, the ECJ invalidated a European Commission decision that had generally facilitated transfer of data between Europe and the United States by providing blanket protection under so-called "Safe Harbor" principles negotiated with the United States Department of Commerce.[115] The plaintiff is an Austrian citizen who had a Facebook account with Facebook's subsidiary in Ireland, and whose data were apparently subject to transfer from Ireland to the United States by Facebook. He complained that the U.S. Safe Harbor principles did not provide sufficient assurances for the protection of his personal data upon transfer, citing in particular the June 2013 disclosures by Edward Snowden. The ECJ agreed, noting in particular that the Safe Harbor rules appeared to be subject to overbroad exceptions permitting access to transferred data by security and law enforcement officials in the United States, and because the United States provided insufficient opportunities to the owners of such data to obtain redress against such intrusions. The actual effect of this ruling is complicated; the extent to which it will actually inhibit trans-Atlantic transfers of data and possibly disadvantage U.S.-based ISPs, such as Facebook, remains to be seen.[116] But it is impossible to read the decision without anticipating a negative reaction to a blanket permission permitting U.S. authorities to obtain any and all data stored in Europe, without even providing notice that they are doing so, in any case where an entity that has access to such data is subject to U.S. jurisdiction—the same position requested by the prosecutor in this case.

The approach presented here allows for efficient service of non-controversial SCA "warrants", when their application appears to be purely domestic or where identifiable U.S. interests clearly predominate, while providing a mechanism for ISPs like Microsoft to show that, in a particular case, there is a treaty process, which is the more appropriate procedural device because of the apparent legitimate interest of the host country and its history of compliance with applicable cooperation treaties or agreements. Whatever solution is eventually adopted in the Second Circuit will be judged by the rest of the world on how well it conforms to comity and the principles of international law.

115. Case C-362/14, Maxmilillian Schrems v. Data Protection Commissioner, InfoCuria (Oct. 6, 2015), *available at* http://curia.europa.eu/juris/document/document.jsf?text=&docid=169195&doclang=en.

116. *See* Dr. Thomas Schurrle, et al., Debevoise & Plimpton, LLP, Transfers of Personal Data to the United States: European Court of Justice Rules the Safe Harbour Protocol Is Potentially Invalid (2015), http://www.debevoise.com/insights/publications/2015/10/transfers-of-personal-data-to-the-united-states.