Texas Law Review
See Also
Volume 95

Article

Data Extraterritoriality

Kristen E. Eichensehr*

INTRODUCTION

Data's intangibility poses significant difficulties for determining where data is located. The problem is not that data is located *nowhere*,[1] but that it may be located *anywhere*, and at least parts of it may be located nearly *everywhere*. And access to data does not depend on physical proximity.

These implications of data's intangibility challenge traditional international law on jurisdiction. International jurisdictional rules rest in large part on States' sovereignty over a particular territory and authority

* Assistant Professor, UCLA School of Law. For helpful comments and conversations, I am grateful to Zach Clopton, Rebecca Ingber, Kal Raustiala, Richard Re, Jennifer Daskal, and participants in the *Texas Law Review* symposium on *Tallinn 2.0*. Thanks to Danielle Hesse for excellent research assistance and to the editors of the *Texas Law Review* for their editorial work.

1. *Cf.* David R. Johnson & David Post, *Law and Borders—The Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367, 1378 (1996) (proposing "conceiving of Cyberspace as a distinct 'place' for purposes of legal analysis by recognizing a legally significant border between Cyberspace and the 'real world'"). As the rest of this Essay will illustrate, the challenge is not that data is outside all jurisdictions, but rather that it is, or may be considered to be, inside many of them.

over people and things within it, and they presuppose that the location of people and things are finite and knowable.[2] The era of cloud computing—where data crosses borders seamlessly, parts of a single file may exist in multiple jurisdictions, and data's storage location often depends on choices by private companies[3]—raises new and difficult questions for States exercising enforcement authority, companies receiving requests from law enforcement agencies, and individuals seeking to protect their privacy.

The *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*[4] builds on the tremendous success of the original *Tallinn Manual*, which focused on restating international law applicable to cyberwarfare.[5] In turning to issues below the use-of-force threshold, *Tallinn 2.0* undertakes an even more ambitious task because it addresses issues that occur more frequently than those included in the original *Manual* and that are the subject of active debate between States.

This Essay addresses *Tallinn 2.0's* rules and commentary on the

2. Scholars have documented the many ways in which data challenges traditional notions of territorial borders as meaningful bases for regulation and enforcement. *See, e.g.*, Zachary D. Clopton, *Data Institutionalism: A Reply to Andrew Woods*, 69 STAN. L. REV. ONLINE 9, 13 (2016) (noting the indeterminacy of existing approaches to extraterritoriality when applied to data); Zachary D. Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45, 46 (2016) (arguing that "[t]echnology weakens territoriality as a proxy for policy goals because data often move in ways that are disconnected with the interests of users and lawmakers" and because "[t]echnology makes it easier for public and private actors to circumvent territorial rules (often without detection)"); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 378–79 (2015) (arguing that data challenges "territoriality doctrine" because, *inter alia*, "the arbitrariness, instability, and location independence of data and its users challenge the assumption that data location should determine the rules that apply" and "the location independence between the data and the government agent accessing the data creates the possibility of actors in State A searching or seizing data in State B without any readily apparent violation of State B's territorial integrity"); Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1083–86 (2017) (arguing that law enforcement's use of network investigative techniques to investigate crime on the dark web poses serious issues regarding extraterritorial enforcement jurisdiction); Orin S. Kerr, *The Fourth Amendment and the Global Internet*, 67 STAN. L. REV. 285, 303 (2015) (arguing in the context of Fourth Amendment doctrine that "Internet technologies . . . disrupt[] the prior relationship between person and place"). *But see* Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 735 (2016) (arguing that "jurisdiction over cloud-based data has nearly everything to do with territoriality," with the result that "the same piece of data may be subject to a number of different jurisdictions at the same time").

3. *See, e.g.*, GOOGLE, *Data and Security*, https://www.google.com/about/datacenters/inside/data-security/index.html [https://perma.cc/2XHW-VJA3] ("Rather than storing each user's data on a single machine or set of machines, we distribute all data . . . across many computers in different locations" and "chunk and replicate the data over multiple systems to avoid a single point of failure").

4. TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS (Michael N. Schmitt ed., 2017) [hereinafter TALLINN MANUAL 2.0].

5. TALLINN MANUAL ON THE INTERNATIONAL LAW APPLICABLE TO CYBER WARFARE (Michael N. Schmitt ed., 2013).

international law governing jurisdiction. The Essay focuses in particular on the *Manual*'s treatment of extraterritorial jurisdiction. Part I first describes the *Manual*'s rules and commentary on extraterritorial jurisdiction. Section I.A then raises a procedural objection to the *Manual*'s approach, namely that ongoing debates about how to determine data's location make the law too unsettled for a restatement project. Section I.B takes on its own terms the *Manual*'s entry into the debate over how to determine data's location and highlights several concerns with and questions raised by the *Manual*'s approach. In light of the critiques set out in Part I, Part II offers some preliminary thoughts on how to make progress in resolving conflicting international claims to jurisdiction over data going forward.

I. Data Location and Territorial Limits

The jurisdictional rules the *Tallinn Manual* sets out are fairly straightforward restatements of existing international law. In Rule 8, the *Manual* explains that "[s]ubject to limitations set forth in international law, a State may exercise territorial and extraterritorial jurisdiction over cyber activities,"[6] making cyberspace jurisdiction analogous to non-cyberspace jurisdictional issues.[7] Rule 11 on "Extraterritorial enforcement jurisdiction" states that "enforcement jurisdiction over cyber infrastructure, cyber activities, and persons who engage in such cyber activities is generally limited to the territory of the State that is exercising the jurisdiction . . . ,"[8] but it recognizes that a state may "exercise extraterritorial enforcement jurisdiction in relation to persons, objects, and cyber activities on the basis of: (a) a specific allocation of authority under international law; or (b) valid consent by a foreign government to exercise jurisdiction on its territory."[9]

The problems arise from attempting to apply Rule 11. Data's intangibility creates complexities for assessing territoriality, as the *Manual*'s drafters acknowledge.[10] The drafters begin by declaring that "international law does not address . . . with clarity" instances where it is "impossible or difficult to reliably identify the State in which digital evidence or other data . . . resides."[11] The drafters nonetheless go on to adjudicate the territoriality and extraterritoriality of several situations where

6. TALLINN MANUAL 2.0, *supra* note 4, at 51.

7. *See also id.* at 55 (discussing territorial jurisdiction); *id.* at 60 (discussing extraterritorial prescriptive jurisdiction).

8. *Id.* at 66–67; *cf.* RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES §§ 431–32 (1987) (addressing "Jurisdiction to Enforce" and "Measures in Aid of Enforcement of Criminal Law").

9. TALLINN MANUAL 2.0, *supra* note 4, at 66.

10. *Id.* at 69 (noting that "determining whether enforcement jurisdiction is territorial or extraterritorial can be complex in the cyber context").

11. *Id.* at 68.

the data storage location is known. They conclude that when a State "access[es] electronic data that is publicly available, such as that on the Internet," but "hosted on servers located abroad," the State is "exercising territorial, as opposed to extraterritorial, enforcement jurisdiction based on the fact that the data is publicly available in their State."[12] The drafters also conclude that a State exercises territorial, not extraterritorial, enforcement jurisdiction when State officials access "data that can be accessed on the Internet, but is not publicly available, such as the content of closed online forums" or content "hidden in the so-called 'dark web,'" "so long as the data is meant to be accessible from the State concerned."[13] The drafters give a specific example of what they believe is permissible under this principle: "If . . . a State's law enforcement agency is able to obtain, under false pretences, the log-on credentials to a closed online forum hosted on servers located abroad, but meant to be accessible to one or more users from the State," the State exercises "territorial enforcement jurisdiction when it accesses the forum from its own territory."[14]

The *Manual*'s drafters distinguish these cases from instances in which "data is not meant to be made available to individuals in the State," such as data on a private computer abroad that is connected to the Internet but not meant to be accessible.[15] Access to that computer would be extraterritorial.[16] Thus, the drafters acknowledge that hacking into a suspected criminal's computer in another State would be extraterritorial enforcement.[17]

The *Manual*'s adjudication of these examples rests on the idea that if data located abroad is "meant to be accessible" from a particular State (or from *every* State for that matter) then the State's access to it is territorial, not extraterritorial. As a practical matter, this means that law enforcement or other State authorities can then access data stored abroad so long as they comply with their own State's laws, whatever they may be.

The *Manual*'s dependence on whether data is "meant to be accessible" as the determining factor in a territoriality assessment poses a procedural problem and raises several substantive concerns. Section I.A discusses the procedural issue, while Section I.B raises questions about the substance of the *Manual*'s test.

12. *Id.* at 69.
13. *Id.*
14. *Id.* at 70.
15. *Id.*
16. *Id.*
17. *Id.* at 68, 70.

A. The Unsettled Law of Cross-Border Data Access

The procedural problem is that the *Manual*'s stated purpose is "to be a reflection of the law as it existed at the point of the *Manual*'s adoption"[18]—to be "an objective restatement of the *lex lata*."[19] But it is impossible to "restate" areas of law that are unsettled. And how to determine whether data is territorial or extraterritorial is an unsettled issue.[20] Questions about data territoriality and extraterritoriality vis-à-vis the United States have spawned a vigorous academic debate in the past several years,[21] but the debate is not just academic. It's also unsettled in state practice.

The Second Circuit's recent decision in *Microsoft Corp. v. United States* highlights the ongoing debate about how to determine data's location.[22] Pursuant to the Stored Communications Act (SCA),[23] the U.S. government served a warrant on Microsoft, ordering the company to produce the contents of the web-based email account of one of its customers.[24] Microsoft provided the non-content information about the account that was stored in the United States,[25] but refused to comply as to the account's contents because the content information was stored in a datacenter in Dublin.[26]

Microsoft acknowledged that it could access the contents of the email account from the United States,[27] but argued that doing so would be an impermissible extraterritorial search and seizure. From Microsoft's perspective, the relevant location for determining whether the warrant was territorial or extraterritorial was the location of the data, not the location of those who access it.[28] Here, the data was located in Dublin, and therefore, even though Microsoft officials in the United States could access the data, compliance with the warrant would constitute impermissible extraterritorial

18. *Id.* at 2.

19. *Id.* at 3. The *Manual*'s drafters take pains to note that the *Manual* "does not represent 'progressive development of the law'" and that they "assiduously avoided including statements reflecting *lex ferenda*. *Id.*

20. The *Manual*'s move into *lex ferenda* on the "meant-to-be-accessible" issue is evidenced by the fact that the *Manual*, which is typically careful to cite the sources of law on which it relies, provides no citations for paragraphs that rely on the "meant-to-be-accessible" theory. *See id.* at 69–70.

21. *See supra* note 2 (collecting sources).

22. 829 F.3d 197 (2d Cir. 2016), *petition for cert. filed*, (U.S. June 23, 2017) (No. 17-2).

23. 18 U.S.C. § 2703 (2012).

24. *Microsoft Corp.*, 829 F.3d at 200.

25. *Id.*

26. *Id.* at 204.

27. *Id.* at 203.

28. *See* Brief for Appellant at 32, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2014 WL 7004807 (arguing that "[t]he search and seizure occur where the evidence is, not where the agent sits").

enforcement of U.S. law, absent consent by Ireland.[29] And Ireland didn't consent. It filed an amicus brief noting its interest in "potential infringements by other states of its sovereign rights with respect to jurisdiction over its territory"[30] and highlighting its willingness to use the U.S.–Ireland Mutual Legal Assistance Treaty to assist the U.S. government in processing the warrant.[31]

The U.S. government, on the other hand, argued that the warrant did not require extraterritorial action. The government focused on Microsoft's control over the requested information,[32] and argued that the warrant "simply requires Microsoft to disclose to law enforcement agents (in the United States) records under its control—regardless of where those records are stored."[33] Because Microsoft controls the requested content, the government argued, "[t]he fact that Microsoft happens to store records responsive to the Warrant overseas does not render the SCA 'extraterritorial' . . . ."[34]

The Second Circuit sided with Microsoft.[35] The court's determination about where the warrant's execution would occur was part of its determination about the presumption against extraterritoriality with respect to the SCA. The presumption against extraterritoriality instructs that "[a]bsent clearly expressed congressional intent to the contrary, federal laws will be construed to have only domestic application."[36] In applying the presumption to the SCA, the Second Circuit first determined that "Congress did not intend the SCA's warrant provisions to apply extraterritorially."[37] It then moved on to determine whether the "conduct relevant to the statute's

29. *Id.* at 33 (arguing that execution of the warrant would violate the "fundamental principle of international law that a 'state's law enforcement officers may exercise their functions in the territory of another state only with the consent of the other state.'" (citing RESTATEMENT (THIRD) OF THE FOREIGN RELATIONS LAW OF THE UNITED STATES § 432(2) (1987)).

30. Brief of Ireland as Amicus Curiae Supporting Appellant at 1, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985); *see also* Mark Scott, *Ireland Lends Support to Microsoft in Email Privacy Case*, N.Y. TIMES (Dec. 24, 2014), https://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case/ [https://perma.cc/2HTM-UTGR] (summarizing the Irish brief). For an analysis of foreign governments as amici in U.S. courts, see Kristen E. Eichensehr, *Foreign Sovereigns as Friends of the Court*, 102 VA. L. REV. 289 (2016).

31. Brief of Ireland as Amicus Curiae Supporting Appellant, *supra* note 30, at 4.

32. Brief for the United States at 31–32, Microsoft Corp. v. United States, 829 F.3d 197 (2d Cir. 2016) (No. 14-2985), 2015 WL 1139654 ("The relevant inquiry . . . concerns the extent of a U.S. court's power to compel Microsoft, a U.S. company, to disclose records in its possession, custody, and control.").

33. *Id.* at 32.

34. *Id.*

35. *Microsoft Corp.*, 829 F.3d at 201–02.

36. RJR Nabisco, Inc. v. European Cmty., 136 S. Ct. 2090, 2100 (2016).

37. *Microsoft Corp.*, 829 F.3d at 216.

focus occurred in the United States"—a territorial application—or abroad—an impermissible extraterritorial application.[38] The court concluded that "[b]ecause the content subject to the Warrant is located in, and would be seized from, the Dublin datacenter, the conduct that falls within the focus of the SCA would occur outside the United States."[39] Execution of the warrant therefore would be extraterritorial.[40] The United States sought en banc review of the panel decision, but the Second Circuit denied the request by an equally divided vote.[41]

The *Tallinn Manual*'s statements about extraterritoriality are in substantial tension with the *Microsoft* decision. The *Manual*'s analysis of extraterritoriality would support the U.S. government's position in the case—a position the Second Circuit rejected.[42] The customer email account that the government ordered Microsoft to disclose was "meant to be accessible" from the United States in that Microsoft maintained access from its U.S. headquarters to the content information stored abroad.[43] The *Manual* takes the position that when data that is meant to be accessible in a State is then accessed in the State, such action counts as territorial enforcement, not extraterritorial enforcement, as the Second Circuit held.[44]

Moreover, the *Manual* also takes the position that "the mere fact that a person or private entity bears a State's nationality does not alone afford that State the legal authority to engage in an exercise of extraterritorial enforcement jurisdiction with respect to that data."[45] The *Manual*'s drafters "hastened to add, however, that the State may exercise enforcement jurisdiction over the individuals or private entities themselves if they are located in the State."[46] That's what happened with Microsoft. The nationality of the individual whose email account the government requested was unknown (at least to the Second Circuit),[47] but Microsoft's presence in

38. *RJR Nabisco*, 136 S. Ct. at 2101.

39. *Microsoft Corp.*, 829 F.3d at 220.

40. *Id.* at 221.

41. Of the eleven active Second Circuit judges, three were recused, leaving eight judges voting on en banc review; of the eight voting judges, four filed dissents from the denial of rehearing en banc. Microsoft Corp. v. United States, 855 F.3d 53, 54 & n.* (2d Cir. 2017) (order denying reh'g en banc).

42. The divergence between the views of the court and the executive branch raises interesting issues as to how to determine the content of U.S. state practice for purposes of customary international law. *See* Ingrid Wuerth, *International Law in Domestic Courts and the* Jurisdictional Immunities of the State *Case*, 13 MELB. J. INT'L L. 819, 821–23 (2012) (discussing differing approaches to state practice when a State's executive and judiciary disagree).

43. TALLINN MANUAL 2.0, *supra* note 4, at 69.

44. *Id.* at 70.

45. *Id.*

46. *Id.*

47. *Microsoft Corp.*, 829 F.3d at 230 (Lynch, J., concurring in the judgment) ("[W]e do not

the United States was used to render it subject to the warrant pursuant to the SCA. The Second Circuit, of course, determined that Microsoft's presence in the United States was insufficient and instead focused on the location of the data. On this point as well, the *Tallinn Manual* would have disagreed, siding with the U.S. government.

The Second Circuit's *Microsoft* opinion will not be the last word on the data territoriality/extraterritoriality issue, even in the United States.[48] Since the Second Circuit denied en banc review at the end of January, lower courts outside the Second Circuit have disagreed with that court's reasoning. In cases involving warrants served on Yahoo and Google for data stored worldwide, magistrate judges have held that the warrants do not reach extraterritorially because the companies will access the data from the United States.[49] Importantly, even these cases, which are more consonant with the *Tallinn Manual*'s approach, do not articulate the "meant-to-be-accessible" standard the *Manual* employs. They focus instead on objective facts about the location of the service provider, rather than an analysis of intent.

My point in highlighting the tensions between the *Manual* and the *Microsoft* case and between the *Microsoft* majority and the recent lower court opinions is not to take a definitive side in this debate as a normative matter. These are complicated issues that are beyond the scope of this Essay.[50] These cases, however, show that the law on how to determine whether access to data is territorial or extraterritorial is unsettled, even within the United States. That's a problem for a manual whose stated aim is to be a restatement of existing law. Rule 11 on extraterritorial enforcement jurisdiction does restate settled law, but the predicate of what

---

know the nationality of the customer.").

48. The United States has asked the Supreme Court to review the case. *See* Petition for Certiorari, United States v. Microsoft Corp., No. 17-2, (U.S. June 23, 2017).

49. *See, e.g.*, In the Matter of the Search of Content That Is Stored at Premises Controlled by Google, No. 16-mc-80263, 2017 WL 1487625, at *1 (N.D. Cal. Apr. 25, 2017) (holding that an SCA warrant ordering Google to disclose data stored worldwide "is a domestic application of the SCA"); In the Matter of the Search of Premises Located at: [redacted]@yahoo.com, Stored at Premises Owned, Maintained, Controlled, or Operated by Yahoo, Inc., No. 6:17-mj-1238 (M.D. Fla. Apr. 7, 2017) (holding that requiring Yahoo to produce data stored worldwide does not involve an extraterritorial application of the SCA because "the focus of [the SCA] is on compelled disclosure, and the compulsion takes place in the United States"); *In re* Info. Associated with One Yahoo Email Address That Is Stored at Premises Controlled by Yahoo, Nos. 17-M-1234 & 17-M-1235, 2017 WL 706307, at *3 (E.D. Wis. Feb. 21, 2017) (holding that SCA warrants issued to Yahoo and Google for data stored worldwide did not "implicate extraterritoriality concerns" because "what matters is the location of the service provider"); *In re* Search Warrant No. 16-960-M-01 to Google, Nos. 16-960-M-01 & 16-10610M, 2017 WL 471564, at *11 (E.D. Pa. Feb. 3, 2017) (holding that because Google will search and the government will review the data in the United States "[t]hese cases . . . involve a permissible domestic application of the SCA").

50. These issues have warranted multiple articles. *See, e.g.*, *supra* note 2 (collecting articles).

is extraterritorial in the context of access to data is the key issue. And on that question, the *Manual* is ahead of its time. The experts who drafted the *Manual* agreed among themselves on a test for assessing extraterritoriality and applications of that test that remain up for grabs even within the United States.

B. New Questions About an Existing Debate

Setting aside the question of whether the law on data extraterritoriality is too unsettled to restate, the *Manual*'s proposed standard of determining territoriality based on whether data is "meant to be accessible" from a particular State raises a number of questions.

First, the *Manual*'s "meant-to-be-accessible" standard raises the question: meant *by whom* to be accessible? The *Manual* doesn't say, and different answers produce significantly different outcomes. In the *Microsoft* case, for example, if, as assumed above, access in the United States would be territorial if either Microsoft *or* the account holder meant the data to be accessible from the United States (as Microsoft did), then the U.S. government would prevail under the *Manual*'s standard. If, however, the *Tallinn Manual* would require the account holder or the account holder *and* Microsoft to mean for the data to be accessible in the United States, then the outcome would depend on the intent of the account holder. The *Manual* doesn't clarify whether the account holder's intent is required, much less how to determine that intent if it is.

Relatedly, the *Manual* does not appear to place any temporal limit on when data is "meant to be accessible" from a particular State. If a potential defendant has a cloud-based email account, stored on servers outside the United States, but intended the account to be accessible during the visit to the United States several years ago, is that sufficient? What about meaning for the same account to be accessible *if* the potential defendant travels to the United States at some unspecified point in the future? Does the mere fact of creating a Gmail, Amazon, or iTunes account suffice to show that the account holder means for the account to be accessible worldwide? The fact that such accounts can be accessed from any computer is, of course, one of their most attractive features. Cloud computing has banished the days when the death of one's personal computer hard drive meant the loss of personal information.

Finally, the implications of the *Manual*'s emphasis on whether data is "meant to be accessible" are not clear for certain, fairly common examples of cross-border data access. The *Manual* says that a State's access to "data that is stored on a private computer abroad, even if connected to the Internet, that is not meant to be accessible" from the State would be

extraterritorial enforcement.[51] As an example, the *Manual* says that if a State hacks into a suspected criminal's computer in another State, the hacking State exercises extraterritorial enforcement jurisdiction, and must therefore have "the latter State's consent or a specific allocation of authority under international law."[52] Consider, however, this example: a Chinese company has an employee in the United States and allows the employee to use a Virtual Private Network to access information on the corporation's servers in China. The data on the corporate network in China is therefore "meant to be accessible" from the United States, but only by the corporation's employee in the United States. Does the *Manual*'s test mean that U.S. government access to the corporate network in China is not extraterritorial? Or consider a U.S. citizen who travels abroad and has a remote desktop program installed so that she can continue to access her home computer while traveling. Does that mean that wherever the citizen travels, whatever country she is in can access her data stored in the United States because it is meant to be accessible to an individual (the U.S. citizen traveler) in that country, and therefore is not extraterritorial? These scenarios pose important questions, especially for companies or other entities that routinely have employees traveling around the world.

As commentators and judges have highlighted, determining territoriality or extraterritoriality based solely on location of the service provider who will access the data *or* the location of the data itself are problematic. But the *Tallinn Manual*'s entry into the fray creates additional complications and uncertainties of its own. An approach more reflective of the current state of things might have been simply to say, as the *Manual*'s drafters do with respect to data whose location is unknown,[53] that there is no settled law to restate.

II. An International Process for International Jurisdiction

Litigants, judges, scholars, and the *Tallinn Manual* itself have proposed numerous different tests to determine whether access to data is territorial or extraterritorial. One test is the location of the data itself, as Microsoft urged.[54] Another is the location where the data is accessed, as the U.S. government argued.[55] Yet another approach would establish a test that takes into account the nationality of the target of the investigation,[56] or the

51. TALLINN MANUAL 2.0, *supra* note 4, at 70.

52. *Id.*

53. *See supra* note 11 and accompanying text.

54. *See supra* notes 27–29 and accompanying text.

55. *See supra* notes 32–34 and accompanying text.

56. *See* Microsoft Corp. v. United States, 829 F.3d 197, 230 (2d Cir. 2016) (Lynch, J., concurring in the judgment) (arguing that it would be "remarkably formalistic to classify" as

nationality and location of the target.[57] Still another approach would rely on a "totality of the circumstances" evaluation to determine extraterritoriality.[58] And finally, the *Tallinn Manual* suggests that the determinative factor is whether data is "meant to be accessible" from the State that wishes to access the information.

Each of these approaches is subject to critique,[59] and the remainder of this Essay does not aim to resolve which test is the best—or even the least worst.[60] Instead, this Part highlights an issue of process, rather than substance: the way forward on data extraterritoriality must be an international one.

In his concurrence in the judgment in the *Microsoft* panel opinion, Judge Gerard Lynch rightly highlighted the problem of reciprocity. He noted that while "[i]t will often be tempting to attempt to protect American interests by extending the reach of American law and undertaking to regulate conduct that occurs beyond our borders," doing so can "cause tensions with . . . other countries, most easily appreciated if we consider the likely American reaction if France or Ireland or Saudi Arabia or Russia proclaimed its right to regulate conduct by Americans within our borders."[61] In other words, whatever rule the U.S. government advocates when it is the

---

extraterritorial a circumstance in which "the American government is demanding from an American company emails of an American citizen resident in the U.S., which are accessible at the push of a button in Redmond, Washington, and which are stored on a server in Ireland only as a result of the American customer's misrepresenting his or her residence, for the purpose of facilitating domestic violations of American law, by exploiting a policy of the American company that exists solely for reasons of convenience and that could be changed . . . at the whim of the American company").

57. Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issue*, 8 J. NAT'L SEC. L. & POL'Y 473, 493 (2016) (describing an agreement under negotiation between the United States and the United Kingdom pursuant to which the United Kingdom could make direct requests to U.S. service providers for "the content of communications of targets that reside outside the United States, and are not U.S. citizens or legal permanent residents" and the United States would have reciprocal rights to make direct requests to U.K. service providers).

58. Microsoft Corp. v. United States, 855 F.3d 53, 60 (2d Cir. 2017) (Carney, J., concurring in the denial of reh'g en banc) (suggesting that courts might "reach a result that better reconciles the interests of law enforcement, privacy, and international comity" if they were freed to determine extraterritoriality based on "the totality of the relevant circumstances," such as "the residency or citizenship of the client whose data is sought, the nationality and operations of the service provider, the storage practices and conditions on disclosure adopted by the provider, and other related factors").

59. *See, e.g.*, Daskal, *supra* note 2, at 390–91 (highlighting problems with both sides' positions in the *Microsoft* case); *supra* Section I.B (discussing problems with the *Tallinn Manual*'s standard).

60. I hope to tackle the broader normative questions in future work on extraterritoriality and cyberspace.

61. Microsoft Corp. v. United States, 829 F.3d 197, 225 (2d Cir. 2016) (Lynch, J., concurring in the judgment), *rhr'g en banc denied*, 855 F.3d 53 (Mem.) (2d Cir. 2017).

data requester, it must be prepared to accept when other governments request the data of U.S. citizens from U.S. providers. The same is true for every country in the world.

To address this issue, Judge Lynch calls on Congress to amend the SCA.[62] But that is not enough. Even if Congress were to amend the SCA, as Judge Lynch suggests, to embody a "more nuanced [rule] than the position advanced by either" the United States or Microsoft,[63] such an act of self-restraint by the United States would not prevent other governments from taking a broader approach. In fact, several governments have begun to do just that.[64]

Self-restraint by the United States and other important countries may have a demonstration effect, encouraging other countries to follow the lead of influential early movers. But countries would be under no obligation to do so or to continue to do so. The temptation to engage in unilateral assertions of power to access data worldwide may be spurred by frustration with existing Mutual Legal Assistance Treaty (MLAT) processes. MLATs are widely viewed as inadequate tools for evidence-gathering both because of long delays in processing of assistance requests[65] and because use of the treaties requires the requesting country to know where data is stored—an increasingly untenable requirement.

A new international agreement or agreements on cross-border data access to permit, but impose legal restrictions on, governments' demands for information from service providers in other countries are the best means of remedying these concerns. New treaty regimes along these lines have been suggested,[66] but they have rightly garnered skepticism as implausible

62. *Id.* at 231–32 (Lynch, J., concurring in the judgment).

63. *Id.* at 231 (Lynch, J., concurring in the judgment).

64. *See, e.g.*, Jennifer Daskal, *Congress Needs to Fix Our Outdated Email Privacy Law*, SLATE (Jan. 26, 2017), http://www.slate.com/articles/technology/future_tense/2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html [https://perma.cc/8UUU-76SM] (discussing extraterritorial data disclosure claims by Belgium and the United Kingdom); Susan Hennessey & Chris Mirasola, *Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?*, LAWFARE (Mar. 27, 2017, 11:02 AM), https://www.lawfareblog.com/did-china-quietly-authorize-law-enforcement-access-data-anywhere-world [https://perma.cc/H27D-BMBU] (reporting that 2016 regulations authorize Chinese law enforcement officials to access digital data through "remote network inspections" anywhere in the world, pursuant only to Chinese domestic law restrictions).

65. *See, e.g.*, Daskal, *supra* note 57, at 475–76 (describing the MLAT process and attendant delays).

66. *See, e.g.*, Brad Smith, *Time for an International Convention on Government Access to Data*, DIGITAL CONSTITUTION (Jan. 20, 2014), https://digitalconstitution.com/2014/01/time-international-convention-government-access-data/ [https://perma.cc/B853-PPUD] (arguing that "unilateral action outside [the MLAT] system . . . is not the best path forward" and that instead countries should negotiate a new treaty to "facilitat[e] timely access to data while ensuring appropriate privacy protections for individuals"); Rep. of the Special Rapporteur on the Right to

in the short term.[67] Considering a broad-based international treaty regime as an end goal, rather than a starting point, may be a more promising way forward.

In the immediate term, the incremental expansion and amendment of existing cybercrime treaties may be a realistic aim.[68] The leading cybercrime treaty is the Council of Europe Convention on Cybercrime, known as the Budapest Convention.[69] Although its membership is open to States beyond the Council of Europe, its 53 states parties are overwhelmingly European and Western, with a few outliers like Japan, Israel, Senegal, and Sri Lanka.[70] In recent years, other regional groups have negotiated the Arab Convention on Combating Information Technology Offences[71] and the African Union Convention on Cyber Security and Personal Data Protection,[72] which has not yet entered into force.[73]

Each treaty requires States to criminalize certain cybercrime

---

Privacy, Joseph A. Cannataci (Special Rapporteur), U.N. Human Rights Council, A/HRC/34/60 at 18 (Feb. 24, 2017), www.ohchr.org/EN/HRBodies/HRC/RegularSessions/Session34/Documents/A_HRC_34_60_EN.docx (proposing a new treaty that would create an "international body tasked with—and granted the authority to authorise—international access to data").

67. *See, e.g.*, Daskal, *supra* note 57, at 492–93 (criticizing Brad Smith's proposed treaty, *see supra* note 66, as "more of a textbook solution than something that could realistically be put in place, at least in the short-term").

68. In 2016, the United States and United Kingdom reportedly undertook negotiation of a bilateral agreement pursuant to which each country could make direct requests to service providers in the other country for wiretaps or stored data of the requesting country's nationals. *See* Ellen Nakashima & Andrea Peterson, *The British Want to Come to America – with Wiretap Orders and Search Warrants*, WASH. POST (Feb. 4, 2016), https://www.washingtonpost.com/world/national-security/the-british-want-to-come-to-america—with-wiretap-orders-and-search-warrants/2016/02/04/b351ce9e-ca86-11e5-a7b2-5a2f824b02c9_story.html [https://perma.cc/Y622-5PRR]; *see also* Daskal, *supra* note 57, at 493 (endorsing an approach like the reported U.S.–U.K. agreement). The current status of the negotiations in the Trump Administration is unclear.

69. Council of Europe, Convention on Cybercrime, *opened for signature* 2001, E.T.S. No. 185, (entered into force 2004) [hereinafter Budapest Convention].

70. *Chart of Signatures and Ratifications of Treaty 185*, COUNCIL OF EUROPE, https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=96wpgBCT [https://perma.cc/AHV9-ZJNT].

71. League of Arab States, Arab Convention on Combating Information Technology Offences, Dec. 21, 2010 [hereinafter Arab League Convention].

72. African Union, Convention on Cyber Security and Personal Data Protection, June 27, 2014, EX.CL/846(XXV), *available at* https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf [hereinafter African Union Convention].

73. *See id.* art. 36 (specifying that the treaty requires 15 ratifications to enter into force); *see also* African Union, List of Countries Which Have Signed, Ratified/Acceded to the African Union Convention on Cyber Security and Personal Data Protection, https://www.au.int/web/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf (showing several signatures but no ratifications to date).

offenses.[74] But they also include provisions that obligate states parties to adopt procedural measures to facilitate investigations and to engage in international cooperation.[75] In the Budapest Convention, for example, the scope of the procedural provisions extends beyond just the cybercrimes each party is required to criminalize pursuant to the treaty, and also reaches "other criminal offenses committed by means of a computer system" and "the collection of evidence in electronic form of a criminal offense."[76] The Council of Europe has begun to address cross-border data access issues under the auspices of the Cybercrime Convention Committee's Cloud Evidence Group.[77] In reports, the Cloud Evidence Group has highlighted the difficulties of applying a territorial framework based on the location of data, and instead suggested the need for a "common international solution" centered on "the location of the person in possession or control of the data" or "[t]he location of the victim at the time of the crime."[78] More recent reports suggest that the Cybercrime Convention Committee is beginning work on an Additional Protocol to the Budapest Convention on cross-border data-access issues.[79]

The regionalization of the cybercrime treaties is less than ideal,[80] but the development of non-European cybercrime conventions in recent years at least shows an appetite for addressing cybercrime and related issues in some areas of the world that have largely remained outside of the Budapest

74. *See* African Union Convention, *supra* note 72, arts. 29–30; Arab League Convention, *supra* note 71, arts. 5–19; Budapest Convention, supra note 69, arts. 2–11.

75. *See* Budapest Convention, supra note 69, arts. 14–34; Arab League Convention, *supra* note 71, arts. 22–42. The relevant provisions in the African Union Convention are less robust than those in the Budapest and Arab League Conventions. *See* African Union Convention, *supra* note 72, arts. 28, 31(3).

76. Budapest Convention, supra note 69, art. 14(2).

77. Cloud Evidence Group, COUNCIL OF EUROPE, http://www.coe.int/en/web/cybercrime/ceg [https://perma.cc/J657-Q9WX] ("The Cloud evidence group explores solutions on criminal justice access to evidence stored on servers in the cloud and in foreign jurisdictions, including through mutual legal assistance.").

78. Council of Europe, *Final Report of the T-CY Cloud Evidence Group, Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY*, paras. 46–47, T-CY (2016)5, (Sept. 16, 2016), *available at* https://rm.coe.int/16806a495e [https://perma.cc/ZCS6-SLTM].

79. *See* Thorbjørn Jagland, Sec'y-Gen., Council of Europe, Remarks at Octopus Conference on Cybercrime, Special Session 15th Anniversary Budapest Convention on Cybercrime, (Nov. 16, 2016), http://www.coe.int/en/web/secretary-general/speeches-2016/-/asset_publisher/TQ9ylWpDFtLP/content/octopus-conference-on-cybercrime-special-session-15th-anniversary-budapest-convention-on-cybercrime [https://perma.cc/VQZ8-KSDM] (discussing Cloud Evidence Working Group's recommendation to negotiate an additional protocol to the Budapest Convention and suggesting that work on the additional protocol will begin by mid-2017).

80. *Cf.* Kristen E. Eichensehr, *The Cyber-Law of Nations*, 103 GEO. L.J. 317, 359 (2015) (discussing U.S. insistence on the Budapest Convention as the main international vehicle for addressing cybercrime and the objections of non-European states to this approach).

Convention framework. Moreover, the similarity between the Budapest Convention and the Arab League Convention in particular suggests that developments in the Council of Europe might be picked up in other regional treaty systems.

On the other hand, the inclusion of additional provisions on transnational evidence-gathering is likely to further alienate countries like Russia and China from the existing treaty regimes. Both countries have expressed opposition to the limited cross-border data access regime that is already included in the Budapest Convention on the grounds that it does not sufficiently respect State sovereignty.[81] Recently, however, even Russia and China have expressed some support for cross-border cooperation on technology-related crimes and investigations. The U.N. Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security—a group that includes China, Russia, and the United States among others—agreed in a 2015 report that States should consider cooperating "in a manner consistent with national and international law with requests from other states in investigating [information and communications technology]-related crime."[82]

International treaties rarely provide quick fixes to any international problem, and the difficult issues surrounding cross-border data access will not be an exception. But at least work is beginning.

III. Conclusion

Tallinn 2.0 is an ambitious effort to tackle some of the most difficult, contested, and frequently occurring issues related to cyberspace, and it will undoubtedly serve, like *Tallinn 1.0* before it, as an invaluable resource for States and commentators going forward. In its effort to cover as much

81. *See generally* Joint Statement, China Inst. of Contemporary Int'l Relations (CICIR)—Ctr. for Strategic & Int'l Studies (CSIS), Bilateral Discussions on Cooperation in Cybersecurity, Ctr. for Strategic & Int'l Stud., at 3 (June 2012), https://www.csis.org/programs/technology-policy-program/cybersecurity/china-institute-contemporary-international [https://perma.cc/Y66N-FTCJ] (noting that representatives from CICIR, in discussing the Budapest Convention, pointed out "inevitable concern over violation of sovereignty and incompatibility with domestic legislations caused by transnational collection of evidence"); Mark Ballard, *UN Rejects International Cybercrime Treaty*, COMPUTER WKLY. (Apr. 20, 2010), http://www.computerweekly.com/news/1280092617/UN-rejects-international-cybercrime-treaty [https://perma.cc/2WK6-KSRM] (noting Russia's opposition to the Budapest Convention provision that allows law enforcement authorities from one state to access computers in a second state with the permission of the computer owner, and without consulting governmental authorities in the second state).

82. U.N. General Assembly, Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security, U.N. Doc. A/70/174, para. 17(e), http://www.un.org/ga/search/view_doc.asp?symbol=A/70/174 [https://perma.cc/FL3N-89E9].

ground as possible, however, the *Manual* may have tried to settle too much, too fast, declaring over and done debates that States are still hashing out. In entering the debate about how to determine data's location for jurisdictional purposes, the *Manual*'s proposed "meant to be accessible" standard raises many new and fundamental questions of its own. However, the *Manual* is undoubtedly correct to consider questions about data's location as a matter of international law. Only a coordinated international solution can solve the puzzle of reconciling intangible data and territorial borders.