2020

Transnational Government Hacking

Jennifer C. Daskal
American University Washington College of Law, jdaskal@wcl.american.edu

Transnational Government Hacking

Jennifer Daskal*

Introduction

Cyber investigations often involve devices and data that cross or are located across international borders. This raises challenges for law enforcement which often finds itself limited by enforcement jurisdiction that stops at its territorial borders. What happens when law enforcement is seeking to access data or a device and the location is unknown? What about situations in which law enforcement has its hands on a device, but the data being accessed via that device is located in another state's jurisdiction? What if the device itself is located overseas—in a jurisdiction unwilling or unable to aid the investigation?

The United States addressed these issues, in part, in 2016 amendments to Federal Rule of Criminal Procedure 41. The updated rule now specifies that a judge can issue a remote access search warrant if the location of the device or data is in a location unknown and its location has been concealed via technological means. This provision provides an additional exception to the otherwise applicable geographic limits on judicial authority to issue search warrants.[1]

In the lead-up to the rule change, several commentators noted, often with concern, that this could lead U.S. governmental officials to inadvertently search and access data and devices in foreign jurisdictions. One commentator suggested that this could yield "the largest expansion of extraterritorial enforcement jurisdiction in FBI history."[2] Others warned that the unilateral accessing of extraterritorially-located data and devices could "put U.S. law enforcement agencies at risk of violating th[e] binding rule of sovereignty, as well as the principle of comity."[3]

Some have further noted—correctly—the criminal law risks presented by extraterritorial investigatory activities that involve non-consensual entry into foreign-located computer systems. Such actions could result in U.S. law enforcement

* Professor, American University Washington College of Law. Special thanks to Gary Corn, Ashley Deeks, Jonathan Mayer, Cedric Yehuda Sabbah, Michael Stawasz, and the participants at the 2019 Cyber Symposium sponsored by the Journal of National Security Law & Policy and Third Way for helpful conversations, suggestions, and input. An additional thanks to my outstanding research assistant Daniel de Zayas.

1. Fed. R. Crim. P. 41(b)(6).

2. *See* Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 Stan. L. Rev. 1075, 1081 (2017); *see also* Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, Just Security (Sept. 16, 2014, 9:10 AM), https://perma.cc/U52G-MTBP.

3. *See* Joseph Lorenzo Hall, Ctr. for Democracy & Tech., Written Statement Before the Judicial Conference Advisory Committee on Rules of Criminal Procedure at 4 (Oct. 24, 2014), https://perma.cc/6LRG-2QMW; Richard Salgado, Google, Inc., Comments on the Proposed Amendment to the Federal Rule of Criminal Procedure 41 at 3-4 (Feb. 13, 2014), https://perma.cc/L6K2-TN7E (noting that respect for sovereignty precludes law enforcement from exercising enforcement jurisdiction in another nation absent that nation's consent).

being subject to criminal prosecution under the domestic laws of the country in which the data or device is located.[4]

Yet, despite the rhetoric, the Rule 41 amendments are of narrow scope. They only address the very limited situation in which the location of a device or data is *unknown* and has been concealed through technical means. In situations in which a device is *known* to be located extraterritorially, the territorial limits on the U.S. warrant authority continue to apply. U.S. judges lack the authority to issue a warrant to search. Rather, law enforcement is, as a general matter, told to instead employ the mutual legal assistance process and seek the assistance of the government where the data or device is located—irrespective of the foreign government's willingness to cooperate.

Meanwhile, there is a lack of clarity as to the rules that apply—and ought to apply—if law enforcement has access to a device, but then seeks to collect data accessible via the online-connected device. In many cases, the location of the sought-after data will be unknown. Data accessed from the cloud may be located outside of the nation's territorial boundaries, even if accessed via a territorially-located device. This, raises questions as to lawfulness of the search under both domestic and international law.

Governments have adopted divergent approaches. Australia, for example, requires foreign government consent if the accessed data is located extraterritorially—even if the device that is used to connect to the data is in the hands of law enforcement in Australia. If, however, the location of the data is unknown and cannot reasonably be determined, then access can be pursued; consent is not required simply because it is impossible to know who to ask for such consent.[5] Many others, including the United States, do not publicly specify whether and in what circumstances law enforcement can seek direct access if and when the data is known to, or may be, located outside the nation's borders.

The implications for security, privacy, and, in particular, the topic of this symposium—the ability to identify and prevent cybercrime—are significant. After all, law enforcement access to digital evidence can be an important tool in criminal investigations involving digital evidence. But while there has been a fair amount of literature on the related questions as to the geographic reach of what I refer to as "indirect access"—situations in which law enforcement obtains evidence with the assistance of a third party, such as Google, Facebook, or any other third party, rather than accessing data directly—there has been much less written about the jurisdictional challenges that arise when the government is engaged in what I call "direct access" — those steps taken by the government to unilaterally access sought-after data, without the engagement of a third party intermediary.[6]

---

4. *See* Ahmed Ghappour, Comment on the Proposed Amendment to Rule 41 at 7 (Feb. 17, 2014), https://perma.cc/Z5G5-UHAA.

5. Telecommunications and Legislative Amendments (Assistance and Access) Bill 2018 (Cth), s 43A (Austl.), https://perma.cc/YMV5-FSEC.

6. On the indirect access issues, *see, e.g.*, Jennifer Daskal, *Privacy and Security Across Borders*, 128 YALE L.J. FORUM 1029 (2019); Paul Schwartz, *Legal Access to the Global Cloud*, 118 COLUM. L. REV.

The goal of this article is to identify and analyze some of the key unresolved questions. The article starts by examining the current international law rules—or really lack thereof—underlying remote access to devices and data across borders. It then examines various domestic law efforts to regulate the remote accessing of data and devices. And it makes a set of legal and policy recommendations designed to guide law and practice going forward. Specifically, I argue that governments should, as a matter of policy and when reasonably possible, seek consent from foreign governments when accessing devices or computer systems known to be located in a foreign jurisdiction. But I suggest that exceptions may be required to deal with those situations in which location of data is unknown and unknowable; the process of getting consent would unduly jeopardize the investigation or is simply impracticable given things like the rapid mobility of the data being sought. And I suggest that consent should not be required if and when law enforcement has physical access to a device and is merely accessing, via that device, data that automatically downloads from the cloud—even though there is the possibility that some such data may be located out of the investigating country's domestic borders.

A few important notes on scope before I begin:

First, the discussion is focused primarily on the jurisdictional questions. It thus references but does not delve into the critically important, and interrelated, questions regarding the specific procedural and substantive standards that do, and should, apply to such access. These are key, foundational issues. Insufficient protections will make any such direct access illegitimate as a matter of human rights law, no matter what the jurisdictional rules. The specifics, however, are complex, demanding careful thought and analysis that are outside the scope of this short Article.[7]

Second, the analysis assumes the prototypically easy case involving the targeted accessing and copying of data that leaves the relevant data intact and available for others to manipulate. It thus assumes a targeted delivery, localized exploitation, and time-limited execution.[8] But a range of other network investigative techniques also can be employed that can delete or alter data, engage in ongoing surveillance, and spread vulnerabilities across systems. In addition, tools that are meant to exploit vulnerabilities in a targeted, limited way can be

1681 (2018); Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018); Andrew Keane Woods, *Litigating Data Sovereignty*, 128 YALE L.J. 328 (2018); *Commission Staff Working Document, Impact Assessment Accompanying Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters and Proposal for a Directive of the European Parliament and of the Council Laying Down Harmonised Rules on the Appointment of Legal Representatives for the Purpose of Gathering Evidence in Criminal Proceedings*, COM (2018) 225 final (Apr. 17, 2018) [hereinafter *EC Impact Assessment*], https://perma.cc/AJ69-WJ2M; Peter Swire & Jennifer Daskal, *What the CLOUD Act Means for Privacy Pros*, INT'L ASS'N PRIVACY PROF'LS. (Mar. 26, 2018), https://perma.cc/33HH-WDSG.

7. *See* SVEN HERPIG, A FRAMEWORK FOR GOVERNMENT HACKING IN CRIMINAL INVESTIGATIONS (2018) (discussing the key issues); Jonathan Mayer, *Government Hacking*, 127 YALE L.J. 570 (2018).

8. *See* Mayer, *Government Hacking*, *supra* note 7, at 583-90 (discussing how government malware is deployed, including the various phases of deployment).

mishandled, misappropriated, or result in unintended consequences.[9] Technological, procedural, and substantive safeguards and protections are needed to address those risks. Situations in which law enforcement employs exploits designed to alter or destroy data, devices, or systems or engage in ongoing surveillance raise additional legal and policy concerns and considerations outside the scope of this article.

Third, the discussion of international law requirements is and should be understood as just that—a narrow analysis of what international law requires. This analysis is distinct from an evaluation of best practices and policy. As I discuss further in Part III, there are a range of policy and practical reasons why states should, as a matter of domestic law, place limits on extraterritorial access to data or devices, even if international law does not require it. Put simply, international law is important, but it is not the only guiding factor. Thus, the discussion of what international law allows should be read as separate from an analysis of what governments *should* permit.

I. INTERNATIONAL LAW

It is a longstanding principle of international law that one state cannot engage in non-consensual law enforcement actions in another state. As a result, State A cannot send agents into State B to seize evidence for law enforcement purposes absent State B's consent. Doing so is generally understood to violate State B's sovereignty and is not permitted under international law.[10] This rule makes sense. The idea of, say, Russian law enforcement agents unilaterally and surreptitiously sneaking into a home in Chicago to seize allegedly stolen art is creepy. And it is rightly understood as an international law violation as a result—one that would trigger the right of the United States to take proportionate countermeasures in response.

Conversely, spying across borders is also generally understood to be permitted or at least not prohibited under international law.[11] Espionage can, and almost always does, violate domestic law. But perhaps out of recognition that everyone

9. Interview by Sharon Driscoll with Riana Pfefferkorn, Fellow, Ctr. for Internet & Soc'y, Stan. L. Sch. (Sept. 19, 2018), https://perma.cc/C7PR-49TL.

10. *See, e.g.*, Corfu Channel (U.K. v. Alb.), Judgment, 1949 I.C.J. Rep. 4, 34-35 (Dec. 15) (rejecting argument that non-consensual evidence gathering in another state is permitted and therefore justifies a violation of territorial sovereignty); S.S. Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10, at ¶ 45 (Sept. 7) (laying out principle that "failing the existence of a permissive rule to the contrary[, a State] may not exercise its power in any form in the territory of another State").

11. *See* Asaf Lubin, *The Liberty to Spy*, 61 HARV. INT'L L.J. (forthcoming 2019) (excellent discussion of different legal perspectives on the status of spying under international law over time); Ashley Deeks, *Confronting & Adapting: Intelligence Agencies and International Law*, 102 VA. L. REV. 599, 608-10 (2016); Ashley Deeks, *An International Legal Framework for Surveillance*, 55 VA. J. INT'L L. 291, 300-04; *see also* TALLINN MANUAL 2.0 ON THE INTERNATIONAL LAW APPLICABLE TO CYBER OPERATIONS 169-170 n.22 (Michael N. Schmitt ed., 2d ed. 2017) [hereinafter TALLINN MANUAL 2.0] (concluding that there is no international law prohibition of espionage per se); Gary D. Brown & Andrew O. Metcalf, *Easier Said Than Done: Legal Reviews of Cyber Weapons*, 7 J. NAT'L SECURITY L. & POL'Y 115, 116 (2014) (noting a "long-standing (and cynically named) 'gentleman's agreement' between nations to ignore espionage in international law"); Asaf Lubin, *Cyber Law and Espionage Law as Communicating Vessels*, 10 INT'L CONF. ON CYBER CONFLICT 203, 205 (2018).

does it, espionage in the form of intelligence gathering is not explicitly prohibited under international law. Thus, if a Russian agent enters the United States to spy on a Chicagoan for intelligence gathering purposes, it would not, under the prevailing view, be a breach of international law—although the agent would be in violation of the U.S. Foreign Agents Registration Act, among other possible domestic criminal laws.[12] Even those who argue that undercover spies who cross borders violate the territorial integrity of the non-consenting state where they are acting, and thus violate international law, generally agree that "remote" espionage, or surveillance that takes place without the crossing of humans across international borders, is lawful, or at least not prohibited by international law.[13]

This then raises foundational questions about how to categorize the remote accessing of data by law enforcement. What if Russian law enforcement remotely and surreptitiously accesses U.S.-located 0s and 1s of interest without ever leaving Russia—leaving the data unaltered in any way that affects its ongoing manipulation and use? First, as a threshold measure, it is unclear if the Russian is acting territorially, based on where the agent is physically located or extraterritorially, based on where the data is located.

Second, assuming Russia is considered to be engaging in an extraterritorial enforcement action, is it best analogized to the kind of extraterritorial law enforcement actions that are prohibited? Or is it more like espionage and permitted—or at least not explicitly prohibited?

The answers to these questions turn on an assessment of both territoriality and the meaning and status of sovereignty under international law. It is to these questions that I now turn.

A. Territorial or Extraterritorial?

In prior work I have explored what I call the "un-territoriality of data"—namely, the ways in which modern technology challenges basic assumptions as to what is "here" and "there," thereby forcing a rethinking of what is territorial and what is extraterritorial.[14] How one answers these questions matters. Territoriality, after all, has long been, and remains, a key foundational principle underlying an array of international law rules and norms.[15]

But as I argued previously, and as debates about remote access to data exemplify, the ways in which data moves, is stored, and is accessed across territorial borders raise foundational questions as to how to *assess* territoriality. Is territoriality linked to the location of data? The location of the person accessing the

12. *See* 22 U.S.C §§ 611-621 (2018). If, however, coupled with a coercive action, such as, say, destroying the target Chicagoan's office or home, then the actions would rise to the level of a prohibited intervention, thereby triggering the right of countermeasures on the part of the United States.

13. *See* Lubin, *The Liberty to Spy*, *supra* note 11 (describing and critiquing this approach).

14. *See* Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 329 (2015).

15. Contrary to the claims of some, I have never suggested otherwise. *See, e.g.*, Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729, 734 n.20 (2016).

data? The location of the person or entity whose data is being accessed? As the question was posed in a European Commission report dealing with the related issue of indirect access, what are the "connecting factors" that matter?[16]

There are various possible answers to these questions. One perspective is represented by what I refer to as the data territorialists—those who focus on the location of the data as the key basis for asserting territorial control. China is squarely in that camp. As is Russia, albeit in a slightly modified form. A data territorialist approach is implicit in the many calls for data location as a means of asserting or guaranteeing access to data as well as other forms of regulatory control.[17] Even those who ostensibly support the free flow of data exhibit data territorialist tendencies at time. In restricting the transfers of data outside the EU absent a finding of adequate data protection safeguards, the EU, for example, presumes that location of data (whether in or out of the EU) dictates control.[18]

Another approach, as expressed in the *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations*, focuses, for purposes on law enforcement jurisdiction, on where the data is "meant to be accessible from," rather than its actual location.[19] If data is "publicly available"—such as that on the open Internet—accessing of that data is a territorial exercise of jurisdiction, regardless of where the underlying 0s and 1s are located.[20] This position is also reflected in the Council of Europe's Budapest Convention.[21] But the Tallinn Manual goes a step further than what is authorized by the Budapest Convention—applying this rule to non-publicly available information as well. If non-publicly available information, such as the content of chats, closed online forums, or non-indexed Internet hosting services such as Tor, is "meant to" be accessible to at least one

16. *EC Impact Assessment*, *supra* note 6, at 28 n.44.

17. *See, e.g.*, ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE AND THE FREE FLOW OF INFORMATION (2015), https://perma.cc/GJJ2-SJ74. There are a range of different reasons why nations impose such restrictions, some but not all connected to a desire to establish exclusive territorial-based control. *See* Courtney Bowman, *Data Localization Laws: An Emerging Global Trend*, JURIST (Jan. 6, 2017, 9:53 AM), https://perma.cc/JYA2-W3JP.

18. Commission Regulation 2016/679, 2016 O.J. (L 119) 1, art. 48 [hereinafter GDPR]. The United States also adopts a version of data sovereignty with respect to transfer restrictions embedded in the Stored Communications Act, which prohibits U.S.-based providers from disclosing communications content to foreign governments. Unlike the category of data sovereignty I am focused on here, however, the restrictions are not tied to data location. In other words, the restrictions arguably limit such transfers whether the underlying data is held in the United States or not.

19. TALLINN MANUAL 2.0, *supra* note 11, at 69-70 (drafted by leading international law scholars from around the world); *id.* at 2-3 (describing the Manual as a "reflection of the law as it existed at the point of the Manual's adoption," rather than a best practices or progressive policy guide); *see also* Michael N. Schmitt & Liis Vihul, *Sovereignty in Cyberspace: Lex Lata Vel Non?*, 111 AM. J. INT'L L. UNBOUND 213, 214 (2017).

20. TALLINN MANUAL 2.0, *supra* note 11, at 69 ¶ 12.

21. Convention on Cybercrime [hereinafter Budapest Convention], art. 32(a), *opened for signature* Nov. 23, 2001, 10 E.T.S. 185, https://perma.cc/47Q3-SAQW (specifying that "a Party may, without the authorization of another Party. . . access publicly available (open source) stored computer data, regardless of where the data is located geographically").

user in the state, then access is territorial, according to the Tallinn Manual. The location of the underlying data is irrelevant in those situations.[22]

Consistent with this approach, the Tallinn Manual also considers government action to be territorial if law enforcement uses false pretenses to obtain the relevant password and access non-public data accessible to someone in the state's territorial borders. So long as the data was meant to be accessible to *someone* in the state, it does not matter that law enforcement logs onto a site housed on servers located outside the nation's border; the fact that it was not meant to be accessed by the investigating law enforcement agents is irrelevant.[23] If, however, law enforcement is accessing data "not meant to" be made available to anyone in the state, such as the data stored on a personal computer located outside the state, then access is deemed extraterritorial.[24]

According to this dividing line, the accessing of extraterritorially-located data from a territorially-located device is almost always a territorial action. That data is "meant to" be accessed from within the state. By contrast, the remote access of an extraterritorially-located personal device is almost always an extraterritorial action, absent some basis for concluding that the device was meant to be remotely accessible.

As Professor Kirsten Eisensechr has ably articulated, the practical and normative questions raised by this approach are myriad:[25] How does one ascertain what is "meant to" be accessible? "Meant to" by whom—the user, the service provider, or some combination thereof? What about the temporal issues? If a user travels overseas and remotely accesses data while doing so, is it "meant to" be accessible in that location for the time period the person is traveling, into perpetuity, or something in between? And what about the situations in which an overseas employee is given permission to remotely access a company's computer systems, via a remote desktop program or other means? Is law enforcement acting territorially if it remotely accesses that company's overseas networks, simply because a single employee within the state is "meant to" have access?[26] In addition to the range of practical difficulties, it is normatively problematic to base an assessment of territoriality on user intent and actions, particularly in those situations in which most key operations and players are located extraterritorially.

A modified approach—and one that I have long supported in connection with the related debates on indirect access—also focuses on factors other than location of data and proposes a multi-factored assessment that incorporates things like the location and nationality of the target, rather than where data is "meant to" be accessed from.[27] This alternative approach is premised on respect for the

22. TALLINN MANUAL 2.0, *supra* note 11, at 69-70 ¶ 13.
23. *Id*.
24. *Id*. at 70 ¶ 14.
25. *See* Kristen E. Eichensehr, *Data Extraterritoriality*, 95 TEX. L. REV. 145, 150-54 (2017).
26. *Id*. (laying out these and related questions that arise).
27. *See* Jennifer Daskal, *Borders and Bits*, 71 VAND. L. REV. 179 (2018); Jennifer Daskal, Peter Swire & Théodore Christakis, *The Globalization of Criminal Evidence*, INT'L ASS'N PRIVACY PROF'LS. (Oct. 16, 2018), https://perma.cc/FQ8P-ZBLV.

sovereign interest in protecting territorial integrity. But it takes explicit note of the increasing mismatch between the technical infrastructure that spans the globe and the physical borders of nation-states. It is thus premised on a recognition of two key issues:

First, the location of data is increasingly delinked from key sovereign interests, including, importantly, the sovereign interest in securing one's own borders and in protecting the security of one's own nationals and residents. Defending against national security threats can require access to—and at times manipulation of—data that is located extraterritorially. Even local criminal investigations, involving fully local victims, perpetrators, and crime scenes, often depend entirely on data that is located outside one's territorial boundaries. As just one measure, a 2018 European Commission study found that 55% of the data of interest to EU-based law enforcement officials engaged in the investigation and prosecution of domestic crime is held by providers located across territorial borders; much of the relevant data is located extraterritorially as well.[28] As a result, an understanding of territoriality that is linked exclusively to the location of 0s and 1s fails to protect the underlying interest in promoting security, privacy, and other core values and interests that territorial sovereignty is meant to protect.

Second, how one defines what is and is not territorial is itself constructed. The goal is thus to identify the core sovereign interest at stake and assess territoriality in ways that, to the extent possible, maps onto and protects those interests. It means looking at things like the location of the crime and the location and nationality of the target, rather than the location of data, in determining what is and is not a legitimate exercise of the state's law enforcement authorities—and hence what is and is not understood as territorial.

This perspective supports the approach taken in recently enacted legislation in the United States—and now implicitly endorsed by the European Commission in its draft e-Evidence proposals—that the state's relationship to the target of an investigation matters much more than the location of the underlying data. Thus, with respect to the related question of indirect access, U.S. law now specifies that if law enforcement serves a judge-issued warrant or other lawfully-issued disclosure on a third-party company, that company must turn order must turn over all responsive data within their possession, custody, or control, regardless of data location.[29] Yet, the law also explicitly recognizes that such broad authority to search sometimes conflicts with foreign government interests in protecting their own citizens' and residents' data. It thus incorporates a statutory motion to quash

28. *EC Impact Assessment*, *supra* note 6, at 14.

29. *See* Stored Communications Act, Pub. L. No. 99-508, tit. II, 100 Stat. 1848, 1860-68 (1986) (codified as amended at 18 U.S.C. §§ 2701-12); Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018) (enacted) (codified in scattered sections of 18 U.S.C.). Of course, there also must be jurisdiction to compel—meaning the provider has to have a sufficient territorial nexus to the US to support such jurisdiction. *See* Justin Hemmings, Sreenidhi Srinivasan & Peter Swire, *Defining the Scope of 'Possession, Custody, or Control' for Privacy Issues and the Cloud Act*, 10 J. NAT'L SECURITY L. & POL'Y 631 (2020).

if, in certain, albeit limited circumstances, the United States is seeking the data of a foreigner outside the United States and the request creates a conflict with foreign government laws.[30] Here, the key triggering factor is the location and nationality of the investigatory target, rather than the location of the data.[31] The EU's draft e-Evidence Regulation, if enacted, similarly would require providers subject to EU member states' to disclose responsive data, regardless of where the data is located.[32]

By analogy, if law enforcement has physical access over and lawful authority to search a device, the underlying data accessed via that device would not in and of itself turn what would otherwise be a territorial search into extraterritorial one. By contrast, the remote accessing of a device that is itself located across borders would be deemed an extraterritorial search. That said, in both scenarios the remote accessing of a computer network system or device across territorial borders directly by law enforcement raises additional issues that need to be taken into account—issues I return to in Part III.

B. An International Law Violation?

The mere fact that something is extraterritorial does not necessarily make it unlawful as a matter of international law. Instead we now must turn to the second key question: Does the remote accessing of data, a device, or computer network system across borders violate international law?

At a foundational level, international law scholars are currently engaged in a heated debate about territorial sovereignty under international law and its

30. CLOUD Act §§ 103(a), (b) (codified at 18 U.S.C. §§ 2703(h), 2713). This, however, can only be brought in the limited circumstances in which the conflict arises between U.S. and the law of countries with which the United States has a bilateral access-to-data agreement authorized in a separate part of the Act. *See infra*, note 31. As of this writing, that is a null set, although it is expected that an agreement between the United States and the U.K. will go into effect in July 2020. The Act separately includes a rule of construction, making clear that companies can raise common-law motions to quash based on conflict of law concerns in those situations in which the new statutory mechanism is not available, although does not provide any guidance as to how courts are to resolve such claims. CLOUD Act §103(c).

31. A separate part of the CLOUD Act takes a similar tack. It establishes a new mechanism for the United States to enter into bilateral agreements with foreign nations, pursuant to which the partner countries are able to directly demand communications content from U.S.-based service providers, subject to a number of procedural and substantive baseline protections. Yet, here too, the law distinguishes between foreign access to foreigners' data and foreign access to United States' citizen and resident data—permitting foreign government direct access to foreigners' data only. If foreign governments seek U.S. person data, they must continue to make a diplomatic request to the United States, via the mutual legal assistance process, for that data. This reflects an assessment that U.S. rules should govern access to U.S. citizen and resident data, whereas foreign government rules can govern foreign access to foreigners' data. *See* CLOUD Act § 105 (codified at 18 U.S.C. § 2523). For a more detailed analysis, see Jennifer Daskal, *Privacy and Speech Across Borders*, Yale L.J. FORUM 1029; Jennifer Daskal & Peter Swire, *Frequently Asked Questions about the U.S. CLOUD Act*, CROSS BORDER DATA FORUM (Apr. 16, 2019), perma.cc/QWS4-L9C2.

32. *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for electronic evidence in criminal matters*, COM (2018) 225 final (Apr. 17, 2018).

application to cyberspace. Is respect for territorial sovereignty a binding international law rule or a principle upon which other more specific rules are based? If it is a binding rule, at what point is the rule of sovereignty violated? And if not, then the question of line-drawing still exists: When does a cross-border action violate other international law rules, including the prohibition on non-intervention?

For drafters of the *Tallinn Manual*, territorial sovereignty is a binding rule of international law—a position explicitly endorsed by the Government of the Netherlands among others.[33] That said, as the Tallinn Manual recognizes, it is not always simple to determine when such cross-border cyber intrusions cross the line into becoming a sovereignty violation.[34] The Tallinn Manual thus lays out a test for determining whether a particular cyber action violates sovereignty—those that (i) cross a threshold level of intrusiveness, or (ii) interfere with or usurp an "inherently governmental function."[35]

But as the Manual also notes, there is disagreement as to when either of these conditions are met. Among the disputed questions: Do actions that lead to a loss of functionality but do not cause physical damage to the device or infrastructure that houses the data constitute a sovereignty violation? What constitutes an inherently governmental function (a concept the Tallinn Manual asserts is critical but does not clearly define)?[36]

Others take the position that sovereignty is a *principle* that provides a foundational set of norms undergirding other legal rules but is not itself an independent legal rule applicable to cyberspace.[37] This view was expressed by then-U.K. Attorney General Jeremy Wright, in a May 2018 speech:

---

33. TALLINN MANUAL 2.0, *supra* note 11; Letter from Ministry of Foreign Affairs of the Kingdom of the Netherlands, to President of the House of Representatives of the Kingdom of the Netherlands, app. at 2-3 (July 5, 2019) [hereinafter Netherlands International Law Statement], perma.cc/8TRS-DKBZ (concluding that "that respect for the sovereignty of other countries is an obligation in its own right, the violation of which may in turn constitute an internationally wrongful act" and endorsing the Tallinn Manual approach); *see also* Schmitt & Vihul, *supra* note 19; Michael N. Schmitt, *"Virtual" Disenfranchisement: Cyber Election Meddling in the Grey Zones of International Law*, 19 CHI. J. INT'L L. 30, 40, 43 (2018).

34. *See* TALLINN MANUAL 2.0, *supra* note 11, at 19 (noting, in a classically understated manner, that the "precise legal character of remote cyber operations that manifest on a State's territory is somewhat unsettled in international law").

35. *Id*. The Netherlands endorsed this particular test for assessing sovereign violations as well. *See* Netherlands International Law Statement, *supra* note 33.

36. The Manual lists various activities that it considers covered: the manipulation of data that interferes with the conduct of elections, collection of taxes, delivery of social services, conduct of diplomacy, and performance of key national defense activities. *See* TALLINN MANUAL 2.0, *supra* note 11, at 22. Interestingly, the Manual also concludes that intent does not matter. A sovereignty breach occurs even if unintended—if, for example, State A conducts a cyber operation against State B, but the operation inadvertently causes loss of functionality in State C. In that case, State C's sovereignty has been violated by State A, even though State A did not intend such a violation. *Id*. at 24-25.

37. Gary P. Corn & Robert Taylor, *Sovereignty in the Age of Cyber*, 111 AM. J. INT'L L. UNBOUND 207, 207-208 (2017); Eichensehr, *supra* note 25; Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace - Part I*, JUST SECURITY (May 30, 2018) [hereinafter Corn & Jensen, *Part 1*], https://perma.cc/RZ4L-LT6N; Gary Corn & Eric Jensen, *The Technicolor Zone of Cyberspace, Part 2*, JUST SECURITY

> Some have sought to argue for the existence of a cyber specific rule of a "violation of territorial sovereignty" in relation to interference in the computer networks of another state without its consent. . . . But I am not persuaded that we can currently extrapolate from th[e] general principle [of sovereignty] a specific rule or additional prohibition for cyber activity beyond that of a prohibited intervention.[38]

Attorney General Wright went on to emphasize: "The U.K. Government's position is therefore that there is no such rule as a matter of current international law."[39]

For Attorney General Wright and several cyber scholars, cyber actions that cross into the realm of an intervention—generally defined as a coercive action that interferes with the internal affairs of the state[40]—are prohibited. But violations of sovereignty that fall short of an intervention are not international law violations, even if a range of such actions could be, and are, criminalized under states' domestic laws.

In some ways, the scholarly dispute is a distraction. Even those who argue for sovereignty as a binding international rule recognize that there are a range of cross-border cyber-related actions that fall short of interfering with sovereignty. And those who argue that protection of sovereignty is a principle, rather than a binding international law rule, recognize that actions rising to the level of a prohibited intervention violate the law. Line-drawing is needed either way. And depending on how one draws these lines, the two sides may not be as far apart as it might otherwise seem.

That said, the starting point differs significantly for those who view sovereignty as a legally binding obligation and those who argue the need to protect sovereignty is a principle, but not an independent rule. Those who take the sovereignty-as-law position are more likely to find a range of low-level and unconsented-to cyber actions across borders to be unlawful intrusions. They are,

---

(June 8, 2018) [hereinafter Corn & Jensen, *Part 2*], https://perma.cc/54H6-3LSR; *cf*. Daskal, *supra* note 27.

38. Jeremy Wright, U.K. Attorney General, Address at Chatham House Royal Institute for International Affairs: Cyber and International Law in the 21st Century (May 23, 2018).

39. *Id*. France's Ministry of Defense has also weighed in on the issue. *See* France's Minister of Defense, International Law Applied to Operations in Cyberspace, https://www.defense.gouv.fr/content/download/567648/9770527/file/international+law+applied+to+operations+in+cyberspace.pdf. But as Gary Corn points out, despite the many claims to the contrary, France is equivocal as its views, stating that an unauthorized penetration of its systems or effects produced on French territory *may* constitute a breach of sovereignty and that the gravity of any breach will be considered on a case-by-case basis. *See* Gary Corn, *Punching the Edges of the Grey Zone: Iranian Cyber Threats and State Cyber Responses*, JUST SECURITY (Feb. 11, 2020), https://www.justsecurity.org/68622/punching-on-the-edges-of-the-grey-zone-iranian-cyber-threats-and-state-cyber-responses/.

40. *See generally* Philip Kunig, *Prohibition of Intervention*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2008) (defining principle of non-intervention); Katja S. Ziegler, *Domaine Réservé*, *in* MAX PLANCK ENCYCLOPEDIA OF PUBLIC INTERNATIONAL LAW (2013) ("The notion of domaine réservé (reserved domain) describes the areas of State activity that are internal or domestic affairs of a State and are therefore within its domestic jurisdiction or competence.").

after all, legitimately concerned about a wild west of cyberspace in which states can act with impunity across borders and manipulate data in ways that can have practical effects or shape the balance of power, even if they do not involve the use or threat of force.[41]

Conversely, those who deem sovereignty a principle rather than a binding legal rule generally do so in order to enable states to more freely engage in a wider range of unconsented-to cyber actions across state borders. The sovereignty as principle perspective stems, in part, from a recognition that there are a range of situations in which consent is either impractical, infeasible, or both. In the context of law enforcement investigations, for example, consent requirements can risk tipping off the very person who is being investigated. Complex counterterrorism operations may involve data or devices located in multiple countries. In many situations, the location of particular data or a device may be unknown, making ex-ante host state consent infeasible. Such an approach recognizes the messy reality and thus reflects a desire to liberate states from the requirement of host state consent.

C. Sorting it All Out

My goal here is to raise the key considerations, not provide a definitive answer—an effort that would require a tome, or perhaps multiple tomes. In so doing I make three overarching observations.

First, while this essay focuses on law enforcement access to data, the international law rules do not and should not vary based on whether the purpose of the information gathering is for intelligence or evidence gathering. It might be tempting to say that, based on long-standing practice with respect to espionage, that international law permits, or at least does not prohibit, cross-border information gathering for intelligence purposes. And it might be tempting to say, also based on long-standing rules with respect to enforcement jurisdiction that international law prohibits cross-border information gathering for evidence gathering and other law enforcement purposes.

But such a purpose-based test will be almost impossible to implement. It assumes a clear-cut division of intelligence and law enforcement operations that can easily be discerned, where in practice the lines between intelligence gathering and law enforcement are often blurred. Moreover, even when there are relatively clear-cut divisions between law enforcement and intelligence operations, information obtained for one purpose may ultimately be shared and used for another. In such situations, how does one assess purpose? Based on the entity that did the information gathering—an easily manipulated factor? Based on how it is ultimately used—a consideration that raises all kinds of practical complexities, given the inevitable and perhaps lengthy time lag between collection and use?

41. *See, e.g.*, David E. Sanger & Nicole Perlroth, *U.S. Escalates Online Attacks on Russia's Power Grid*, N.Y. TIMES (June 15, 2019), perma.cc/RAV2-VM3K (highlighting the risk of escalatory cyber incursions and counter-responses across borders).

I thus start from the premise that international law rules governing law enforcement access should focus on the nature of state *action* and its effect, rather than the *purpose or intent* of the particular action. This approach also means that while this essay is addressing the international law rules as they pertain to law enforcement, they should be understood as general rules that will have broader application, with implications for intelligence gathering—and, depending on the details, perhaps counterterrorism and other operations as well.

Second, rules that categorically prohibit the non-consensual accessing of 0s and 1s in another nation's borders fail to protect the key sovereign interests at stake—interests that are often delinked to the location of 0s and 1s. Such rules give states undue veto power based simply on the fact that third parties have decided to host data in their jurisdiction, even in situations in which the nation has no articulable interest in the data other than the fact that it is physically located within the nation's borders.

Third, as a result, rules should be designed to reflect this reality. Those who view sovereignty as a principle rather than a binding rule provide the greatest flexibility to design the rules that better reflect the key interest at stake—in an array of different areas, not just with respect to law enforcement. But a similar flexibility could also be achieved by recognizing sovereignty as a binding rule, but then defining sovereignty in a way that is tied to a range of factors delinked from the location of 1s and 0s. No matter what the starting point, a state should not be at risk for violating international law any time they engage in the non-consensual accessing of data across borders, particularly in situations in which the state is seeking the data of one of its residents or citizens, pursuant to lawful process, and the data happens to be located extraterritorially, located within the borders of a state that has no cognizable interest in the data other than the fact that relevant data happens to be housed within its territory.[42]

Fourth, any approach, whatever the starting point, should be coupled with the articulation of and commitment to baseline procedural and substantive human rights standards that govern the accessing of evidence, wherever located. This is critical to avoid what are the legitimate fears of a free-for-all in which nations can act with impunity across borders and the standards devolve to the least common denominator. Establishment and promotion of these baseline human rights standards support nations' own sovereign interests as well.

Fifth, and finally, it is worth nothing that sovereignty itself is an amorphous concept—one that means different things to different actors. As Professor Louis Henkin put it close to a decade ago, albeit in a different context, "The meaning of 'sovereignty' is confused and its uses are various, some of them unworthy, some

42. *See, e.g.*, Corn & Taylor, *supra* note 37; Daskal, *supra* note 27; Eichensehr, *supra* note 25; Corn & Jensen, *Part 1*, *supra* note 37; Corn & Jensen, *Part 2*, *supra* note 37.

even destructive of human values."[43] As Henkin also put it: "[W]e would do better than we are doing, if we saw in the tatters of our sovereignty not obstacles, not as pretext for indifference, for isolationism, but responsibility and opportunities to secure human values."[44] Whatever the approach taken, there is a need to establish clear red lines, norms of behavior, and responsibilities. Invocation of sovereignty, whether as a principle or a rule, does not answer the hard questions that need to be addressed.

II. DOMESTIC LAW: KEY INITIATIVES & OPEN QUESTIONS

A range of countries have adopted, or are in the process of adopting, domestic laws that authorize and set preconditions on the issuance of remote access warrants.[45] Conversely, most domestic laws prohibit the unauthorized accessing of data and devices within their borders. This creates an obvious conflict of laws. Absent bilateral or multilateral agreement, the remote accessing of data or devices by law enforcement risks violating the domestic laws of where the data or device is located.

This section briefly examines the approaches of three jurisdictions—Australia, the United States, and the U.K.—as well as that endorsed in the Council of Europe's Cybercrime Convention. These are hardly the only possible approaches, nor are they the only countries and entities considering these issues. They are chosen nonetheless because they reflect an interesting sampling that highlights some of the key considerations and challenges.

A. Australia

Legislation enacted by Australia in 2018 authorizes the issuance of so-called covert "computer access warrants"—enabling law enforcement to, among other things, remotely access data and devices.[46]

As the legislation recognizes, sometimes sought-after data or devices will be located territorially and sometimes extraterritorially. If Australian law enforcement is accessing a device or data known to be located in a foreign country, law enforcement must first obtain consent of that foreign country. Absent such advance consent, the resulting evidence is inadmissible in Australian

43. *See* Louis Henkin, *That "S" Word: Sovereignty, and Globalization, and Human Rights, Et Cetera*, 68 FORDHAM L. REV. 1, 1 (1999).

44. *Id*. at 14.

45. *See* Telecommunications and Legislative Amendments *(Assistance* and *Access) Act 2018* (Cth) sch 2 pt 1 div 4 para 87 (Austl.), https://perma.cc/G68R-V25X; COUNCIL OF EUROPE CYBERCRIME CONVENTION COMMITTEE (T-CY), AD-HOC SUB-GROUP ON JURISDICTION AND TRANSBORDER ACCESS TO DATA, TRANSBORDER ACCESS AND JURISDICTION: WHAT ARE THE OPTIONS?, T-CY (2012)3, 29-42 (Dec. 6, 2012), https://perma.cc/S3XM-L597 (describing various European initiatives and approaches).

46. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, at sch. 2 pt 1 div 4 para 87.

court.[47] If, however, the location of the data is unknown or cannot be reasonably determined, foreign government consent is not required.[48] The legislation does not specify what happens if initially the location is unknown, but then later it is determined to be located extraterritorially.

Notably, the consent requirement applies with respect to both devices located across territorial borders and to devices held territorially, when the data is located across territorial borders. Thus, even if the device is in the hands of Australian law enforcement operating within Australia, but data accessed via that territorially-located device is known to be stored on a server outside of Australia, Australian law enforcement must obtain foreign government consent.[49]

Interestingly, the same legislation takes a different tack when dealing with indirect access. Specifically, the legislation explicitly authorizes law enforcement to serve technical assistance warrants on companies that are located outside of Australia's borders—so long as they provide services or products used by Australians—without imposing any sort of foreign government consent requirement.[50] These assistance warrants, in turn, can require providers to take steps that will assist in the gathering of data, without limitation to the location of the data.[51]

The legislation thus adopts a dichotomy with respect to the treatment of direct and indirect access. Direct access requires strict attention to and limits based on the location of the underlying data or device. Indirect access does not. So long as the provider serves Australians, the provider is obliged to disclose—or take action with respect to—accessible data, regardless of the location of the data. I return to this distinction in Part III.

B. The United States

In the Unites States, judges can, pursuant to the 2016 amendments to Federal Rule of Criminal Procedure 41, issue a remote access search warrant if the location of the device or data is in a location *unknown* and the location has been concealed via technological means. If, however, a sought-after device is *known* to be located extraterritorially, judges have no authority to issue such warrants.

As discussed above, these amendments were the subject of significant controversy. A primary concern was that judges would inadvertently authorize warrants

47. *Id*.; Explanatory Memorandum, Telecommunications and Other Legislation Amendments (Assistance and Access) Bill 2018 (Cth) paras 591-98 (Austl.) [hereinafter *Explanatory Memo, Austl. Assistance & Access Bill*], https://perma.cc/8KF2-452L (explaining situations in which consent is needed).

48. As the explanatory note makes clear, there may be "frequent[]" situations in which this is the case, and the location of data is unknowable or indeterminable. *Explanatory Memo, Austl. Assistance & Access Bill*, *supra* note 47, at paras 597-98.

49. *Id*. at para 592.

50. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, 2018, sch 1, part 15, ss 317C, 317L (Austl.); Explanatory Document, Telecommunications and Other Legislation Amendments (Assistance and Access) Bill 2018 (Cth) 9 (Austl.) https://perma.cc/92J6-6W2Y [hereinafter *Austl. Assistance & Access Bill Explanatory Document*].

51. Telecommunications and Legislative Amendments (Assistance and Access) Act, *supra* note 45, 2018, sch 1, part 15, ss 317C, 317L.

to search and seize data or devices located extraterritorially. This was presumed to be a breach of international law.[52] But, notably, these remote search warrants can only be issued in those situations in which the location is unknown and the location has been concealed via technical means. If the device is known to be located outside the United States, or if the location is unknown but has not been concealed and thus there is still an opportunity to figure it out, then judges lack the authority to issue such warrants. As discussed in Part II, it is not at all evident that this kind of access does, or should, violate international law; at the very least, international law is entirely unsettled on this point.

In contrast to the Australian legislation, U.S. law does not explicitly address the additional and more controversial set of issues—whether and in what circumstances courts can issue warrants for extraterritorially-located data accessible from territorially-located devices. This is uncharted territory. On the one hand, a recent U.S. Supreme Court decision suggests, without specifying, that the territorial reach of the search turns on the location of the underlying data—an approach presumptively would make the accessing of extraterritorially-located data outside the scope of a warrant. On the other hand, a range of Circuit court cases involving wiretaps suggest that the underlying location of data is irrelevant, so long as it is accessed on a territorially-held device.

Specifically, in the case of *Riley v. California*, the U.S. Supreme Court indicated, albeit based on a very different set of facts, that the location of the data being sought was key to assessing the territoriality, and thus permissible scope, of the search. In *Riley*, officers seized a device from a suspect incident to arrest. The U.S. rules on search incident to arrest generally allow officers to thoroughly search the property recovered from an arrestee's person. Yet, the Court set limits in the context of searching digital evidence, prohibiting the search of a recovered cell phone. As the Court put it: "[O]fficers searching a phone's data would not typically know whether the information they are viewing was stored locally at the time of the arrest or has been pulled from the cloud."[53] The Court elaborated: To authorize such a search would, in the Court's view, "be like finding a key in a suspect's pocket and arguing that it allowed law enforcement to unlock and search a house."[54]

The permissible scope of the search thus turned, at least in part, on the location of the underlying data. While it might be permissible to look at data actually stored on the phone, it was not, according to the Court, permissible to examine data located elsewhere, unless law enforcement obtained a separate warrant to do so. By analogy, the judiciary's territorially-limited warrant authority would be limited to territorially-located data. It would not reach data located extraterritorially, even if accessed from a territorially-located device.

52. *See supra* notes 2-4 and accompanying text.
53. Riley v. California, 573 U.S. 373, 397 (2014).
54. *Id.*

That said, *Riley* dealt with a specific question about the search incident to arrest doctrine and the scope of a warrantless search pursuant to that doctrine. The Supreme Court did not and has not yet weighed in on the question as to whether such a search would be permissible if a warrant had been obtained. In other words, can warrants, which are territorially-limited, authorize the search of data pulled from the cloud, regardless of the location of the data that is being accessed?

In other cases, U.S. circuit courts have suggested that so long as law enforcement has lawful access to a device, it should be able to access information that is reached via that interconnected device, without regard to the location of that information. In several cases, courts have concluded that officers lawfully on the premises of a home can answer a ringing telephone and listen in – irrespective of the location of the speaker on the other end.[55] And in the context of wiretapping, courts have held that the required territorial nexus is satisfied so long as the listening occurs within a judge's territorial jurisdiction, regardless of where the conversation takes place.[56] In at least one case, a court has concluded that the Wiretap Act can, as a result, authorize the listening into a conversation that takes place wholly overseas, on the grounds that the interception took place in the United States.[57]

Meanwhile, Congress has since weighed in, expressing its view that, at least in the related context of indirect access, the location of data is irrelevant for determining territoriality. Pursuant to the CLOUD Act, territorially-located providers are, in response to a compelled disclosure order issued pursuant to the Stored Communications Act, required to turn over all responsive data within their "possession, custody, or control, regardless of whether such [data] is located within or outside of the United States."[58] In the related cases leading up to the CLOUD Act, courts were divided on the issue. The Second Circuit took the position, akin to that suggested in *Riley*, that territoriality depended on the location of data–thus concluding that U.S. law enforcement efforts to compel U.S.-based providers to disclose extraterritorially-located data were an impermissible extraterritorial exercise of the then-applicable statute.[59] But numerous district courts in other jurisdictions disagreed, concluding that territoriality turned on the location of the

55. *See, e.g.*, United States v. Vandino, 680 F.2d 1329, 1335 (11th Cir. 1982) (adopting the view that law enforcement officials, lawfully on the premises, can answer a ringing phone); United States v. Kane, 450 F.2d 77 (5th Cir. 1971) (same).

56. *See, e.g.*, United States v. Henley, 766 F.3d 893, 911-12 (8th Cir. 2014); United States v. Luong, 471 F.3d 1107, 1109-10 (9th Cir. 2006); United States v. Jackson, 207 F.3d 910, 914-15 (7th Cir. 2000), *vacated on other grounds*, 531 U.S. 953 (2000); United States v. Denman, 100 F.3d 399 (5th Cir. 1996), cert. denied, 520 U.S. 1121 (1996); United States v. Tavarez, 40 F.3d 1136, 1138 (10th Cir. 1994); United States v. Rodriguez, 968 F.2d 130 (2d Cir. 1992).

57. United States v. Cano-Flores, 796 F.3d 83 (D.C. Cir. 2015), *cert. denied*, 136 S.Ct. 1688 (2015).

58. CLOUD Act, § 103(a)(1) (codified at 18 U.S.C. § 2713).

59. *In re* Warrant to Search a Certain E–Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2016), *vacated*, 138 S. Ct. 1186 (2018).

provider, and thus efforts to compel U.S.-based providers to turn over extraterritorially-located communications content were permissible.[60]

In sum, the issue as to whether and to what extent U.S. authorities can, pursuant to a warrant, lawfully access extraterritorially-located data from a territorially-located device remains an unsettled area of U.S. law.

C. The U.K.

The U.K. also has passed relatively recent, albeit controversial legislation authorizing, among other things, the issuance of "equipment interference warrants"—namely, warrants that permit l"interference" with computer systems and devices in order to obtain communications content and other data.[61]

The territorial limitations are instructive. Law enforcement chiefs can issue such warrants, but only if "there is a British Islands connection."[62] There is, however, a British Islands connection if "any of the conduct authorised"—including the monitoring, recording, observing, or listening—takes place in the British Isles, "regardless of the location of the equipment that would, or may, be interfered with."[63] Nothing in the law requires foreign country consent where the data or equipment is located.

With respect to indirect access, the same legislation also explicitly authorizes the issuance of warrants requiring the disclosure of non-content data on operators of telecommunication systems outside the U.K., so long as there is sufficient jurisdiction to serve the order. [64] A service provider is, however, excused from compliance if it is not "reasonably practicable" to comply.[65] The legislation specifies that conflicting legal obligations should be taken into account in deciding whether it is reasonably practicable for an extraterritorially-located provider to comply—but nonetheless assumes a broad jurisdiction to compel, at least with respect to non-content data.

In 2019, the U.K. also adopted a new law—the Crime (Overseas Protection Orders) Act 2019, which authorizes judges to issue overseas protection orders requiring extraterritorially-located providers to produce a range of data, including

60. *See, e.g.*, *In re* Search Warrant to Google, Inc., 264 F. Supp. 3d 1268 (N.D. Ala. 2017); *In re* Search Warrant No. 16-960-M-1 to Google, 275 F. Supp. 3d 605, 619 (E.D. Pa. 2017), *aff'g* 232 F. Supp. 3d 708 (E.D. Pa. 2017); *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809, at *5 (N.D. Cal. Aug. 14, 2017), *aff'g* 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); *In re* Search of Info. Associated with [redacted]@gmail.com that is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634, at *27 (D.D.C. July 31, 2017), *aff'g* 2017 WL 2480752 (D.D.C. June 2, 2017); *In re* Search of Info. Associated with Accounts Identified as [redacted]@gmail.com, 268 F. Supp. 3d 1060, 1071 (C.D. Cal. 2017); *In re* Search Warrant to Google, Inc., No. 16-4116, 2017 WL 2985391, at *12 (D.N.J. July 10, 2017); *In re* Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156, at *4 (E.D. Wis. June 30, 2017); *In re* Search of Premises Located at [Redacted]@yahoo.com, No. 17-mj-1238, slip op. at 3 (M.D. Fla. Apr. 7, 2017).

61. Investigatory Powers Act 2016, c. 3, § 99 (UK).

62. *Id.* § 107.

63. *Id.* §§ 99, 107.

64. *Id.* § 85.

65. *Id.* § 66.

content.[66] A precondition to issuing these orders, however, is the existence of an international cooperation agreement permitting the issuance of such orders. In October 2019, the U.K. and United States entered into precisely the kind of agreement that would permit this kind of access—and in fact the Act was written precisely to allow the U.K. to be able to take advantage of the kinds of access provided for by these agreements.[67] Thus, if the U.K. serves a compelled disclosure order on a U.S.-based provider pursuant to this agreement, the U.S.-based provider could be required to disclose data in its possession, custody, or control, regardless of the location of the data. This is a broad assertion of authority, but is premised on consent; there must first be a data-sharing agreement in place.

D. The Cyber Crime Convention

The Convention on Cybercrime takes the position that the direct cross-border accessing of data is permissible in two situations: if the data is publicly available, such as something one can access via a Google search; or if the party receives the consent of the person who has the authority to access and disclose.[68] Otherwise, the Convention presumes strict territorial limits on searches based on the location of both data and devices.

Thus, if, authorities are lawfully searching a computer system, they can examine other data that can be accessed via the initial system—but only if that data is in its territory or the authorities are proceeding with consent.[69] If the data is located extraterritorially, and there is no consent to search, it cannot be accessed, at least according to the scheme laid out by the Cybercrime Convention.

That said, an explanatory note was careful to note that the Convention only addresses those situations in which "all agreed" that such kinds of transborder access is permissible. The Convention leaves many situations unresolved, including the many situations in which the location of data accessed via a territorially-located device or system is unknown and unknowable, as well as situations in which the location of the device or system is itself unknown and unknowable. Subsequent reports by the Convention's so-called Cloud Committee have

66. Crimes (Overseas Productions Order) Act 2019, c. 5 (UK), https://perma.cc/6HJ5-LEN2.

67. *See* Agreement between the Government of the United Kingdom of Great Britain and Northern Ireland and the Government of the United States of America on Access to Electronic Data for the Purpose of Countering Serious Crime, Oct. 3, 2019, U.K.-U.S., C.S. USA No. 6 (2019) (CP 178); Jennifer Daskal & Peter Swire, *The UK-US CLOUD Act Agreement Is Finally Here, Containing New Safeguards*, LAWFARE BLOG (Oct. 8, 2018, 2:33 PM), https://perma.cc/N5R8-HNDV. The agreement does not go into effect until 180 days after being sent to the U.S. Congress, absent formal objection by Congress, pursuant to the expedited procedures laid out in the CLOUD Act.

68. Budapest Convention, *supra* note 21, art. 32.

69. *Id*. art. 19(2).

repeatedly warned that the "loss of (knowledge of) location" often makes the principle of territoriality very difficult to apply.[70]

With respect to indirect access, the Cybercrime Convention, consistent with the practice of state parties, assumes a broader jurisdictional reach. The Convention requires states to pass legislation necessary to empower competent authorities to order any "person in its territory to submit specified computer data in that person's possession or control."[71] Unlike with respect to direct access, there is no explicit limitation with respect to the location of the data. For subscriber information (meaning things like name, IP address, and billing information) the scope is even broader: Any service provide "offering its services in the territory of the Party"—whether physically present or not—can be required to "submit subscriber information relating to such services in that service provider's possession or control."[72] A new draft article would go further, requiring state parties to the convention to set up systems by which State A can issue an order to a provider in State B, requiring the provider to disclose stored subscriber information in its possession and control, regardless of the location of the data.[73]

E. Other Side: Domestic Law Prohibitions On Access

At the same time that several states are seeking or at least considering expanded authorities for remote accessing of devices and data, an array of domestic laws prohibit, and in fact criminalize, the kind of access being pursued. In the United States, for example, an array of different laws come into play, depending on the particular action. The most obvious one is the Computer Fraud and Abuse Act, which criminalizes the unauthorized access to a computer, broadly defined to include most data processing devices and facilities used to store data associated with such devices.[74] Other countries have similar laws. In 2002, Russia filed criminal charges against an FBI agent for alleged unauthorized access to computers of Russians being (ironically) investigated for unlawful hacking.[75] In fact, unauthorized access to computers and related infrastructure is widely recognized and treated as a criminal law violation.

This is a familiar dichotomy with respect to espionage. Espionage is conducted by almost every state—hence its status as permitted, or at least not prohibited,

70. *See* COUNCIL OF EUROPE CYBERCRIME CONVENTION COMMITTEE (T-CY), CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY (Sept. 16, 2016), https://perma.cc/S764-W4NA.

71. Budapest Convention, *supra* note 21, art. 18(1)(a).

72. *Id*. art 18(1)(b).

73. *See Preparation of a 2d Additional Protocol to the Budapest convention on cybercrime* 14-16 (Council of Eur. Cybercrime Convention Comm. (T-CY), Provisional Text, 2019); *see also Budapest Convention and Related Standards*, COUNCIL OF EUR., https://perma.cc/F4V3-QPER (indicating efforts to adopt a new additional protocol).

74. 10 U.S.C. § 1030 (2018).

75. Mike Brunker, *FBI Agent Charged with Hacking*, NBC NEWS (Aug. 15, 2002), https://perma.cc/8JR8-F44Y.

under international law. Yet it is almost always, depending on how it is carried out, a violation of the domestic law where the spying takes place.

III. A WAY FORWARD

This section will tentatively assess the way forward. As described in more detail in what follows, this section operates from the premise that the kind of activity being discussed here—the cross-border accessing and copying of data for law enforcement purposes, without more, does not violate clearly established international law. Thus, the key question is not what does international law require—a framing which takes us down a detour for which there is active debate and no clear-cut answer. Instead the key questions are: what *should* states do as a matter of domestic policy? And what rules, if any, *should* be pursued on an international scale? It is to these normative questions that I now turn.

A. Direct v. Indirect

Every jurisdiction considered in this essay applies slightly different—and more restrictive—standards to direct accessing of data and devices across borders than to indirect access. As a result, a range of laws now explicitly or implicitly require providers to disclose data in their custody or control without regard to data location, whereas the same laws often delimit state access based on the location of the sought-after data or device. This offers some reasons why indirect and direct access are—and should be—treated differently as a matter of domestic policy and law.

First, indirect access incorporates an additional actor, and thus layer of protection, between the compulsory order sought by law enforcement and its ultimate execution and disclosure. While many have expressed a legitimate fear of tech companies being co-opted by the state, the reality is that these same companies can, and do, take steps to protect customer data or resist overreach. In fact, governments regularly complain that companies act in obstructive ways, thwarting access that they deem important.[76] Such companies can and do also raise concerns if and when the request of one government conflicts with laws or obligations of another—something that puts them in the middle of conflicting legal obligations and that they have an obvious incentive to raise and avoid.[77] By contrast, when government actors are doing the searches directly, there is no additional third party to resist or raise concerns regarding a conflict of laws. As a result, conflicting legal rules—and the perspectives of other foreign sovereigns

76. *See* Will Carter & Jennifer Daskal, *Low-Hanging Fruit: Digital-Based Solutions to the Digital Evidence Divide* 18-19, CSIS (July 2018), https://perma.cc/CPM5-ZHZ5.

77. *See, e.g.*, Hof van Beroep [HvB] [Court of Appeal] Antwerpen, 12e ch. Nov. 20, 2013, 2012/CO/1054 (Belg.) (describing history of the case), *translated in* 11 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 137 (2014), https://perma.cc/6UHT-DA7K (discussing challenge raised by Yahoo! based on alleged conflict of laws); Openbaar Ministerie v. Skype Communications SARL, Hof van Beroep [HvB] [Court of Appeal] Antwerp, Nov. 15, 2017, 2016/CO/1006 (Belg.) (discussing challenge raised by Skype based on alleged conflict of laws); Discussion *supra* note 30 (provisions of CLOUD Act that explicitly authorize providers to raise claims based on conflict of laws).

that underlie those rules—may not even be considered, let alone adequately addressed.

Second, pursuant to an indirect access request, providers are being asked to turn over data in their custody or control. Absent data transfer restrictions that create a conflict of laws, providers can and do make data transfers across territorial border with some regularity. Requesting states are, as a result, seeming simply asking private actors to do what they do for all kinds of business and other reasons anyway.

B. Accessing Data from a Territorially-Held Device

For reasons discussed in Part I, the accessing of cloud-stored data that automatically downloads on a territorially-held device does not violate international law. This, in fact, is common ground between those who view sovereignty as a binding rule and those who view sovereignty as a principle rather than a binding international rule.[78] Domestic law rules should track this understanding of international law and permit such access, pursuant to appropriate procedural and substantive safeguards governing access to the device and data located on the device, to include, among other things, post-collection limits on retention, dissemination, and use. But these procedural and substantive protections should apply irrespective of the location of the data. This is true for at least four reasons.

First, it is often not possible to identify the location of data accessed via an Internet-connected device. Some such data may be held on the device itself; some accessed from the cloud; some from within the state's territorial jurisdiction; some from without. Imposition of a location-based limitation on data that is set to automatically download onto a device can be incredibly difficult to implement. In fact, the only way to effectively enforce it would be to impose a categorical bar on connecting and accessing information via the connected device. To extent such a categorical bar is put in place, it should be based on other factors such as the risks to privacy or the security concerns resulting from the access to potentially vast troves on data on the phone – not based on a hypothetical, but difficult to asertain, location-of-data concern.

Second, even if location can be identified, a single device or account may link up to data located in multiple different jurisdictions, including jurisdictions that have absolutely no connection to the investigation other than the fact that sought-after 0s and 1s are held on a server within their territories. Requiring law enforcement to seek consent of each and every country that touches the data as a condition for access may be practically unworkable, at least in a timely manner.

Third, and relatedly, a requirement that law enforcement seek and get consent to access data from a territorially-held device can give foreign jurisdictions with no actual equity in the case undue veto power, without actually protecting any of

78. *See* discussion *supra* Part I.B. In fact, the Tallinn Manual's test for determining the territoriality of law enforcement jurisdiction—whether or not the data was "meant to" be accessible—makes clear that, in the drafters' view, such access does not violate sovereignty or international law. *Id.*

the legitimate equities or interests at stake. The time delays that will inevitably result can lead to the loss of critical information and potentially undermine legitimate investigations. In addition, even if law enforcement knows where the device or data is located, it may be in a place with which the requesting country lacks diplomatic relations, or at least lacks good diplomatic relations. And if even the diplomatic relations are sound, the other country may not have the sophistication, resources, or motivation to act.

Fourth, when a user brings a device into a particular jurisdiction, that user is—or least should be—on notice that the jurisdiction in which he or she is located may seek to access the device, including data that is accessible from the device. This is a very different situation from a user traveling to a foreign country yet deliberately leaving his or her device at home.

In sum, domestic law rules can and should impose robust procedural and substantive limitations on the searches of devices in the government's possession, particularly given the depth and breadth of potentially available information. But these rules should depend on things other than the location of data. For similar reasons, the accessing of extraterritorially located data via a territorially-held device should not be deemed to violate international law.

C. Extraterritorial Accessing and Manipulation of Devices, Infrastructure, or Networks Across Borders

Accessing of devices, infrastructure, or networks across borders raises different considerations. So does the use of a device in hand to send an exploit to access networks and devices in foreign governments in order to access and download data that are not previously set up to be accessed via the device. Such kinds of direct, non-consensual accessing of devices or data raise additional considerations and concerns than the accessing of extraterritorially-located data from a territorially-located device that has been already set up to access that data.

Here too, the international law questions are not clearly established. For those who view sovereignty as a principle rather than a binding international rule, the mere action of accessing and copying data from a device or system located extraterritorially does not violate international law. But even those who view sovereignty to be a rule, rather than a principle also recognize that not all such cross-border access usurps an inherently government function and thereby violates sovereignty. True, there may be times when cross-border access does violate such a function—if for example it interferes in a foreign state's own law enforcement activities. But what if law enforcement officials in State A are seeking data of one of their own citizens in the investigation of a local crime that, for whatever reason, happens to be located on an extraterritorially-located server or device in State B? Absent additional factors, it is hard to conceive of how State B's sovereignty has been violated.

Thus, I turn to what the rules should be—not what they are—and highlight the ways in which direct accessing of a device or system located in a foreign state raises additional concerns not present when law enforcement accesses

extraterritorially-located data from a territorially-held device, in ways consistent with how the territorially-located device has been pre-programmed.

First, in authorizing the cross-border accessing of devices and systems, governments risk violating the domestic law rules in foreign nations, thereby potentially exposing one's agents to criminal liability, as well as international censure. Governments should, as a matter of good policy and sound diplomacy, limit actions that violate other nations' laws.

Second, the user's expectations are different. When a user has his or her device on hand, the user is on notice that the jurisdiction in which he or she is located may seek to access that device and the data accessible to that device. By contrast, the user does not generally think that the device is also subject to foreign government surveillance. And in fact, there is something intuitively creepy about a set of rules that permit states to surreptitiously access data and devices in other countries' jurisdictions. Law and policy should track those user expectations.

Third, and relatedly, rules that give nations free rein to hack into devices and systems in foreign nations creates a free-for-all—with dangerous implications for privacy and security.

Given these considerations, governments should require, as a default rule and matter of domestic law, that law enforcement agents first obtain the consent of the host government before accessing a device, server, or computer system in another state's territorial jurisdiction. Such rules can and should incorporate exceptions for instances in which: (a) the location is unknown and unknowable; and (b) seeking host state consent would unduly risk compromising an important investigation. Additional details need to be worked out. Before concluding that location is unknown, for example, agents should be required to take reasonable steps to identify the location. And in all situations, states should adopt stringent rules and procedures, including a requirement of high-level approval, before allowing law enforcement to proceed with a unilateral search of a device located outside its borders.

Ultimately, this approach should be adopted and incorporated into bilateral and multilateral treaties—thus forming positive international law.

CONCLUSION

Direct access to data across borders can be critical in many criminal investigations. But whereas there has been an increasing amount of discussion about the jurisdictional rules on indirect access—when providers are being compelled to produce extraterritorially-located data—there has been much less discussion as to the appropriate scope and limits of direct access. This essay seeks to jumpstart the conversation and fill the gap—examining the international law rules, analyzing an array of domestic law initiatives, and making tentative legal and policy recommendations for the future. As digital evidence becomes increasingly important to even ordinary criminal investigations, and as the mismatch between our technical infrastructure and state borders grows, a clear articulation of the rules, policies, and practices governing such access will become increasingly important.