Vanderbilt Law Review

Volume 71 | Issue 1 Article 3

2018

Borders and Bits

Jennifer Daskal

Borders and Bits

*Jennifer Daskal**

Our personal data is everywhere and anywhere, moving across national borders in ways that defy normal expectations of how things and people travel from Point A to Point B. Yet, whereas data transits the globe without any intrinsic ties to territory, the governments that seek to access or regulate this data operate with territorial-based limits. This Article tackles the inherent tension between how governments and data operate, the jurisdictional conflicts that have emerged, and the power that has been delegated to the multinational corporations that manage our data across borders as a result. It does so through the lens of the highly contested and often conflicting approaches to the jurisdictional reach of law enforcement over data, the so-called right to be forgotten, and a range of other privacy regulations—engaging in an in-depth analysis as to how these issues are playing out across both Europe and the United States.

In so doing, the Article highlights the flaws with the straightforward application of old jurisdictional rules onto the new medium of data—taking on recent scholarship on this issue. And it shines a spotlight on the unilateral rulemaking by powerful states and the powerful multinational companies that manage our data, which in turn puts private, multinational companies increasingly in control of whose rules govern and thus the substance of both privacy and speech rights on a global, or near-global, basis.

* Associate Professor, American University School of Law; Open Society Institute Fellow (2016–2017). For helpful conversations and input, special thanks to Jonas Anderson; Paul Berman; Cathrin Bauer-Bulst; Anupam Chander; Rebecca Crootof; Daphne Keller; Laura deNardis; Vanessa Franssen; Amanda Frost; Cihan Parlar; Sean Watts; Peter Swire; Andrew Woods; the faculty at William & Mary Law School; the faculty at Tel Aviv University; participants at the 2017 Privacy Law Scholars Conference; my research assistants, Brooke Hofhenke and Eugene Mok; and the terrific editors at the *Vanderbilt Law Review*.

INTRODUCTION

Our personal data is everywhere and anywhere, moving across national borders in ways that defy normal expectations of how things and people travel from Point A to Point B. Yet, whereas data transits the globe without any intrinsic ties to territory, the governments that seek to access or regulate this data operate with territorial-based limits. This basic dichotomy between how governments and data operate is leading to an increasing number of jurisdictional conflicts, incentivizing data localization mandates as a means of asserting territorial control (and thus ensuring access to and regulatory power over sought-after

data), and raising normative questions about how to draw the line between what is territorial and what is extraterritorial in the regulation of a predominantly unterritorial medium.

The key debates are in some ways familiar. As the internet grew in the 1990s, there was a lively dispute between the unterritorialists, such as Professor David Post,[1] and the territorialists, such as Professors Jack Goldsmith and Tim Wu,[2] about whether the internet would defy territorial regulations (the unterritorialists) or whether it would increasingly succumb to longstanding jurisdictional rules and territorial-based controls (the territorialists). History has sided with the territorialists. The new system of international governance that the unterritorialists both predicted and advocated for has not come to pass.[3] To the contrary, states[4] have increasingly found ways to regulate and compel production of data that passes through their borders and to use new technology (such as location-based filtering mechanisms) and new mandates (such as data location requirements) to increase territorial-based controls. This is as Goldsmith and Wu predicted.[5]

But as this Article explores, the cross-border effects of the competing jurisdictional claims are in many ways more contested, fraught, and consequential than Goldsmith and Wu recognized. True, new supranational institutions have not come to exist; rather, territorial-based controls are the norm. But whereas Goldsmith and Wu applauded these developments as promoting decentralized, democratic decisionmaking, the increasingly extraterritorial effects of territorial-based regulation defy this assumption of local, democratic accountability.

Moreover, the debate of the 1990s failed to account for the role of private, third-party providers in setting the rules. Operating alongside the territorial governments—and sometimes displacing them—are the major multinational companies that manage our data. These corporations play an increasingly critical role in mediating disputes across borders and in determining, interpreting, and administering the rules that apply. When Mark Zuckerberg, CEO and cofounder of Facebook, said, "[i]n a lot of ways Facebook is more like a

1. *See, e.g.*, David R. Johnson & David Post, *Law and Borders—the Rise of Law in Cyberspace*, 48 STAN. L. REV. 1367 (1996).

2. *See, e.g.*, JACK GOLDSMITH & TIM WU, WHO CONTROLS THE INTERNET? ILLUSIONS OF A BORDERLESS WORLD (2006).

3. *See* Johnson & Post, *supra* note 1, at 1368, 1372–73 (warning that regulators would "lose their battle to impose local regulations").

4. For the purposes of this Article, I use the term "state" to refer to an independent, sovereign, self-governing political entity that is recognized by the international community as such.

5. *See* GOLDSMITH & WU, *supra* note 2.

government than a traditional company," he was not exaggerating.[6] The multinational companies that manage our data have taken on a form of international governance in ways that traditional governments can't and won't. And while analogies can be made to the power yielded by other multinational corporate operations, such as in the banking, oil and gas, and manufacturing industries, there is something different and profound about the role of private tech companies in setting the scope of our privacy, speech, and associational rights. Whereas the early debates presented a fairly binary choice between territorial governmental control and the development of new supranational entities and norms, the reality that has emerged is much messier and more complicated.

This Article examines these developments through the highly contested and often conflicting approaches to the jurisdictional reach of law enforcement over data, the so-called right to be forgotten, and European Union privacy regulations.[7] Each of these areas is contested, evolving, and highly important to the scope of privacy and speech rights on a global or near-global scale. The scope of cross-border law enforcement jurisdiction has been the source of high-stakes litigation and policy discussions in both the United States and European Union, as well as in numerous other nations. The European Commission, for example, has been tasked with defining jurisdictional norms for determining law enforcement access to data;[8] the state parties to the Council of Europe's Convention on Cybercrime (the "Budapest

6. *See* FRANKLIN FOER, WORLD WITHOUT MIND: THE EXISTENTIAL THREAT OF BIG TECH 61 (2017) (quoting Mark Zuckerberg).

7. There are numerous additional areas where these debates are arising, including, for example, with respect to intelligence surveillance, tax policy, and tort law. *See, e.g.*, CYBERCRIME CONVENTION COMM. (T-CY), COUNCIL OF EUR., CRIMINAL JUSTICE ACCESS TO ELECTRONIC EVIDENCE IN THE CLOUD: RECOMMENDATIONS FOR CONSIDERATION BY THE T-CY: FINAL REPORT OF THE T-CY CLOUD EVIDENCE GROUP 7–8 (Sept. 16, 2016), http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e [https://perma.cc/C5JB-D3U4] [hereinafter CEG REPORT] (describing ways in which a service provider "may be under different layers of jurisdictions for various legal aspects related to its service at the same time"). But the three areas at issue here—law enforcement access to data, regulation of content, and the broader efforts to regulate the treatment of personal data—are themselves sufficiently broad and complex to highlight some of the key, competing pressures and normative interests at stake. Together, they exemplify some of the foundational issues about what constitutes a territorial versus extraterritorial exercise of enforcement or regulatory authority, how to think about the sovereign interests at stake, and the role of third-party intermediaries in resolving or, in some cases dictating, the answers to these questions.

8. *See Council Conclusions on Improving Criminal Justice in Cyberspace*, COUNCIL EUR. UNION 3–5 (June 9, 2016), http://www.consilium.europa.eu/en/meetings/jha/2016/06/Cyberspace—EN_pdf/ [https://perma.cc/D96E-5F4K]. The Commission's non-paper and related technical document was presented in June 2017. *See Improving Cross-Border Access to Electronic Evidence: Findings from the Expert Process and Suggested Way Forward*, EUR. COMMISSION, https://ec.europa.eu/home-affairs/sites/homeaffairs/files/docs/pages/20170522_non-paper_electronic_evidence_en.pdf (last visited Oct. 18, 2017) [https://perma.cc/KA9F-DDK5].

Convention") have adopted a new guidance note and are considering a possible new protocol regarding the appropriate scope of enforcement jurisdiction over certain types of data;[9] and the United States and United Kingdom have negotiated a draft agreement to facilitate access to data across borders, something that the U.K. Deputy National Security Adviser has testified about twice in Congress and that Prime Minister Teresa May has described as one of her top priorities vis-à-vis the United States.[10]

Meanwhile, decisions from courts such as the European Court of Justice regarding the right to be forgotten raise weighty questions about the reach of territorial regulation with extraterritorial effect, such as whose conception of speech rights govern and who decides.[11] The manner in which the right has both been challenged and implemented also highlights both the explicit and implicit power of private corporations to determine the scope of privacy and speech rights and to mediate normative disputes across borders. Broader regulatory efforts in the EU and elsewhere provide additional examples of states seeking to impose their privacy and other related rules on a near-global

---

9. *See* Cybercrime Convention Comm. (T-CY), *T-CY Guidance Note #10 Production Orders for Subscriber Information (Article 18 Budapest Convention)*, COUNCIL EUR. 1–9 (Nov. 15, 2016), https://rm.coe.int/16806f943e [https://perma.cc/3F8N-AFJ6] [hereinafter Cybercrime Convention Comm. Guidance]; *see also* Cybercrime Convention Comm. (T-CY), *(Draft) Terms of Reference for the Preparation of a Draft 2nd Additional Protocol to the Budapest Convention on Cybercrime*, COUNCIL EUR. (June 1, 2017), https://rm.coe.int/-draft-terms-of-reference-for-the-preparation-of-a-draft-2nd-additiona/168071b794 [https://perma.cc/Y25E-3D6K] [hereinafter Cybercrime Convention Comm. Proposal]; *Cybercrime, Towards a Protocol on Evidence in the Cloud*, COUNCIL EUR. PORTAL (June 8, 2017), https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud [https://perma.cc/86U9-RKA2] [hereinafter *Cybercrime*].

10. *See Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era: Hearing Before the H. Comm. on the Judiciary*, 115th Cong. (June 15, 2017) (written statement of Paddy McGuiness, Deputy National Security Adviser, U.K.), https://judiciary.house.gov/wp-content/uploads/2017/06/McGuinness-Testimony.pdf [https://perma.cc/XS6Y-A2DB]; *Hearing Before the S. Judiciary Subcomm. on Crime and Terrorism*, 115th Cong. (May 10, 2017) (written testimony of Paddy McGuiness, Deputy National Security Adviser, U.K.), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf [https://perma.cc/CSK8-MLNX]; *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 9–14 (2016) (statement of David Bitkower, Principal Deputy Assistant Att'y Gen., Criminal Division, Department of Justice), https://www.justice.gov/opa/file/828686/download [https://perma.cc/MU72-LR5U]; 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?utm_term=.b3b046c7c27b [https://perma.cc/4BXU-ADS8].

11. *See* Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD) (*Google Spain Case*) (May 13, 2014), http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&docid=152065&cid=244711 [https://perma.cc/PDU5-VUT7].

scale—again mediated by the major multinational corporations that manage our data.[12]

This Article then draws out the implications from the case studies. Specifically, it identifies and defends three key takeaways that flow from an examination of the key disputes. First, the unique features of data challenge previously relatively stable assessments of what is territorial and what is extraterritorial.[13] And despite the claims of some, these challenges cannot be resolved by simply pointing to preexisting bodies of law (which are themselves contested and unsettled) in analogous areas of intellectual property or money.[14] Or at least they cannot be resolved in a particularly normative and practically satisfying way. The question is not just, "how have others resolved similar issues in loosely analogous situations in the past?" but rather, "how *should* we answer these questions, particularly when such important considerations of personal privacy, individual autonomy, speech rights, and security are at stake?"

---

12. I am hardly the first scholar to explore this phenomenon. *See, e.g.*, Anu Bradford, *The Brussels Effect*, 107 NW. U. L. REV. 1 (2012); Austin L. Parrish, *Reclaiming International Law from Extraterritoriality*, 93 MINN. L. REV. 815 (2009); Gregory Shaffer, *Globalization and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Privacy Standards*, 25 YALE J. INT'L L. 1 (2000). This Article seeks to shine additional light on how this phenomenon is playing out with respect to law enforcement access issues and regulation of privacy rights, including in just the short time since these earlier articles were published.

13. For a sampling of the relevant literature and ongoing debates, see PAUL SCHIFF BERMAN, GLOBAL LEGAL PLURALISM: A JURISPRUDENCE OF LAW BEYOND BORDERS (2012); GOLDSMITH & WU, *supra* note 2; Damon C. Andrews & John M. Newman, *Personal Jurisdiction and Choice of Law in the Cloud*, 73 MD. L. REV. 313 (2013); Jennifer Daskal, *The Un-territoriality of Data*, 125 YALE L.J. 326, 365–78 (2015); Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075 (2017); Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016); and Orin Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?*, 70 STAN. L. REV. ONLINE 58 (2017), https://review.law.stanford.edu/wp-content/uploads/sites/3/2017/07/70-Stan.-L.-Rev.-Online-58-Kerr-Murphy.pdf [https://perma.cc/XJ48-75K3].

14. *Cf.* Woods, *supra* note 13, at 748–66 (asserting that there is nothing particularly unique about the efforts to regulate data). Contrary to Woods' claims, *see* Woods, *supra* note 13, at 755, I do not, and have never, suggested that data falls outside of nation-state—and thus largely territorial-based—attempts to control. In fact, my project over the past several years has been to *define* the jurisdictional reach of domestic law enforcement over the data that they are seeking to access. In other words, I *presume* nation-state, and thus territory-based, efforts to access, regulate, and control data, and seek to think through the nation-states' jurisdictional reach and how the particular features of data challenge those efforts. *See, e.g.*, Jennifer Daskal, *Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues*, 8 J. NAT'L SECURITY L. & POL'Y 473 (2016); Daskal, *supra* note 13, at 365–78; Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Data Fix*, JUST SECURITY (Aug. 1, 2016, 8:03 AM), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/ [https://perma.cc/2AWT-Z5NB]; Jennifer Daskal, *The Microsoft Warrant Case: The Policy Issues*, AM. CONST. SOC'Y FOR L. & POL'Y (Sept. 8, 2016), http://www.acslaw.org/acsblog/the-microsoft-warrant-case-the-policy-issues [https://perma.cc/L9NB-UWAS].

Second, the transnational nature of both data and the companies that regulate our data means territorial regulations are increasingly having an outsized extraterritorial effect, yielding the kind of global or near-global standard-setting that the unterritorialists once predicted, but via local action. This in turn challenges the territorialists' normative defense of such decentralized lawmaking as an example of democratically accountable decisionmaking that promotes self-determination.

Third, and relatedly, this phenomenon is largely being mediated by the private parties that hold and manage our data. It is these companies that increasingly determine whose rules govern and, in key ways, how they are interpreted and applied.[15] In doing so, they set the scope of privacy and speech rights on an international scale. As a result, the key relationship is not between just the governments and the persons that they govern, but instead a set of dynamic interactions between governments, the governed, and the multinational companies that manage our data and mediate between governments. This is a new phenomenon: the role and power of these third-party players were neither anticipated nor accounted for in the more stylized debates of the 1990s. And it is a phenomenon that has significant implications for both substantive and procedural rights.

Two final observations. First, although I focus primarily on how these issues are playing out in the United States and European Union, I do not intend to suggest that these are the only important players. Rather, these are issues being dealt with by just about every nation in the world, with different approaches taken in places like Russia and China than in the United States and European Union.[16] But the United States and European Union provide an important, interesting, and instructive place to start. They are large and powerful actors. And while they sometimes take divergent approaches, they share enough common values and normative assumptions that there is both the possibility and reality of increased harmonization in key areas. They thus make informative case studies.

Second, lest anyone should think that these are just wonky jurisdictional questions that have little import beyond the four corners of conflicts or choice of law textbooks, let me provide a reminder of the implications. In a world where data moves rapidly around the globe, often in ways totally unknown or even unconceivable to the average individual, the answers to these jurisdictional questions often

15. *See infra* Section I.A.

16. I hope and plan in future work to engage in an exploration of how these issues are playing out in a wider range of countries as well.

determine not just government's ability to access or manage data, but the rights and protections that apply. In determining who gets to set the rules, the jurisdictional rules indirectly determine the scope of one's privacy, associational, and speech rights. Put simply, those basic jurisdictional questions have a profound implication for the balance of power. And they matter to our security, to our privacy, to business and economic interests, to citizens' relationship with their governments, to the prospects for democratic accountability, and to our understanding of and ability to shape policy going forward.

I. LAW ENFORCEMENT ACCESS TO DATA ACROSS BORDERS

The question of how to square the territorial-based rules governing law enforcement jurisdiction over data with the unterritorial—and in key ways unique—features of data is a difficult one, and has been the subject of a handful of high-stakes court cases, diplomatic discussions, and policy debates over the past several years.[17] As the Cybercrime Convention's Cloud Evidence Group recently put it, "a major challenge of cloud computing is that data is not stable but often distributed over and moving between different services, providers, locations and jurisdictions, while law enforcement powers are usually defined territorially."[18]

To date, answers to the key jurisdictional questions vary depending on the government seeking to access the data, the type of data at issue, and the perspective of the judges that oversee many of the requests. To complicate matters, several nations prohibit domestic-based providers from disclosing certain locally held data to foreign governments, whereas several (and sometimes the same) nations assert the authority to compel production of data that is extraterritorially located, thereby creating an increasingly potent conflict of laws.

The following highlights some of the different approaches, looking first at law enforcement efforts to access data from the third-party companies that control it, and second, at the related but somewhat different issues that arise when law enforcement itself seeks to directly access data as opposed to compelling a third party to do so.

A. Compelled Disclosure Orders

The question of who has the authority to compel production of data for law enforcement purposes has implications for, among other

17. *See infra* Sections I.A, I.B.

18. *See* CEG REPORT, *supra* note 7, at 17.

things, privacy, security, the future development of the internet, and principles of sovereignty. I start by looking at two very divergent approaches to the scope of permissible compelled disclosure—the location-driven approach, as exemplified by the increasingly disputed approach taken by the Second Circuit in the *Microsoft Ireland* case, and the just-about-anything-is-covered approach taken by the Belgian courts in the Skype and Yahoo! cases. I then turn to the more nuanced efforts to redefine jurisdictional rules in ways that seek to better account for the underlying interests at stake.

1. The Location-Driven Approach: *Microsoft Ireland*

In June 2016, the Second Circuit issued its ruling in the so-called *Microsoft Ireland* case.[19] The case dates to December 2013, when the U.S. government obtained a warrant pursuant to the Electronic Communications Privacy Act ("ECPA"), which compelled Microsoft to turn over data that was located on a server in Dublin, Ireland, but could be accessed by Microsoft employees located in Redmond, Washington.[20] Microsoft objected—arguing that the U.S. government has no authority to demand the production of data located outside the United States' borders.[21] According to Microsoft, this was an impermissible extraterritorial exercise of the government's warrant authority. The government fought back, arguing that Microsoft could access the data from Redmond, Washington, and therefore that this was a territorial, not an extraterritorial, exercise of its authority. The government analogized the warrant to a compelled disclosure order issued pursuant to a subpoena.[22]

Both the magistrate and district court judges sided with the government.[23] But the Second Circuit reversed.[24] The argument proceeded in three key steps. First, the Second Circuit concluded, as both parties agreed, that the ECPA, the underlying statute, did not have extraterritorial effect. Second, the court ascertained the primary

19. *See* Microsoft Corp. v. United States (*In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp.) (*Microsoft Ireland*), 829 F.3d 197 (2d Cir. 2016), *reh'g denied,* Microsoft Corp. v. United States (*In re* Warrant to Search Certain E-Mail Account Controlled & Maintained by Microsoft Corp.), 855 F.3d 53 (2d Cir. 2017) (en banc).

20. *Microsoft Ireland*, 829 F.3d at 200.

21. *Id.* at 209.

22. *See In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014), *rev'd*, *Microsoft Ireland*, 829 F.3d 466; *In re* Warrant to Search a Certain E–Mail Account Controlled and Maintained by Microsoft Corporation, No. 13-MJ-2814, 2014 WL 4629624 (S.D.N.Y. Aug. 29, 2014).

23. *In re Warrant*, 15 F. Supp. 3d at 466.

24. *Microsoft Ireland*, 829 F.3d at 222.

"focus" of the statute as being about protecting privacy.[25] And third, the Second Circuit ruled that the privacy intrusion occurred at the place where the data was located and thus seized—in this case, Ireland.[26]

The Second Circuit thus established the following rule: U.S. law enforcement's authority to compel stored communications content, via a warrant issued pursuant to the ECPA, extends only to data located within the United States. If law enforcement seeks communications content located outside the United States, it needs to make a mutual legal assistance request to the foreign government of the territory where the data is located and await that government's response (or access it by other means). This is so even if the crime, victim, and target of the investigation are all located in the United States. It is so even if the only foreign government link is that the data happens to be held in the foreign government's territory for tax or other economic reasons, such as lower energy costs. And it is so even if there is no way for the government to ascertain the specific location of the data, and thus no clarity about where to direct the request for mutual legal assistance.

As I have written elsewhere, this single-minded focus on data location as determinative of law enforcement jurisdiction is hard to justify even under the court's own reasoning.[27] First, even if the Second Circuit is right that the focus of the statute is on privacy, it is not at all clear that the privacy intrusion occurs in Ireland as opposed to the United States. The United States government is not accessing the data in Ireland; Microsoft is. But Microsoft already has access to the data as its caretaker and in fact moves it around without notice to or control by the user.[28] Any additional privacy intrusion occurs when the data is shared with the U.S. government (which would occur in the United States), not when transferred from Ireland to the United States.[29] This

25. *Id.* at 217, 220–21 (applying the analysis set out by the Supreme Court in Morrison v. Nat'l Austl. Bank Ltd., 561 U.S. 247, 266–70 (2010)). For critiques of the presumption against extraterritoriality, see, e.g., Zachary T. Clopton, *Replacing the Presumption Against Extraterritoriality*, 94 B.U. L. REV. 1 (2014); Anthony J. Colangelo, Essay, *What is Extraterritorial Jurisdiction?*, 99 CORNELL L. REV. 1303, 1323 (2014) (emphasizing that " 'territorial' and 'extraterritorial' are fluid constructs subject to conceptual manipulation"); and William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L. 85, 112–24 (1998).

26. *Microsoft Ireland*, 829 F.3d at 217, 220–21.

27. *See, e.g.*, Jennifer Daskal, *The Dangerous Implications of the* Microsoft Ireland *Case*, JUST SECURITY (Oct. 14, 2016, 1:24 PM), https://www.justsecurity.org/33577/dangerous-implications-microsoft-ireland-case/ [https://perma.cc/7QSP-GX3X].

28. *See, e.g.*, *In re* Search of Info. Associated with [Redacted]@gmail.com, No. 16-mj-00757 (BAH), 2017 U.S. Dist. LEXIS 130153, at *5–7 (D.D.C. July 31, 2017) (emphasizing that email service providers—in this case Google—regularly transfer data from server to server without notice to the user).

29. *See* Jennifer Daskal, *Congress Needs to Fix Our Outdated Email Privacy Law*, SLATE (Jan. 26, 2017, 1:17 PM), http://www.slate.com/articles/technology/future_tense/

is a key point, and one that I will return to later. It highlights, among other things, the increased power of third-party providers in managing personal data and thus determining the rules that apply.

Second, it is not at all clear that the Second Circuit's ruling advances the privacy interests the court seeks to protect.[30] After all, the government proceeded by a warrant based on probable cause. There is no question that the government would have been able to compel disclosure of that data had it been stored in the United States, and that there would be no privacy violation, absent some problem with the warrant. It does not become a privacy violation simply because data moved elsewhere. In fact, the case arguably undercuts, rather than enhances, privacy. The United States now needs to make a diplomatic request for data, via the mutual legal assistance process, every time it seeks data located in a foreign jurisdiction. The relevant foreign government, should it choose to respond, then accesses the data according to its own substantive and procedural standards. But most foreign government rules governing law enforcement access to stored communications content are *less* privacy protective than the United States' requirement of probable cause and independent judicial review.[31] The ruling potentially pushes law enforcement requests—even for U.S. citizens' and residents' data—into less protective systems, simply based on where the data happens to be held.[32]

This data location–driven approach to determining law enforcement jurisdiction also leads to a range of concerning policy implications. Most importantly, it significantly undercuts U.S. law enforcement's ability to access sought-after evidence, even in situations where there is probable cause to do so, and even when the target of the investigation is located in the United States and properly subject to U.S. law enforcement jurisdiction. Rather than directly accessing data from

---

2017/01/the_confusing_court_case_over_microsoft_data_on_servers_in_ireland.html [https://perma.cc/D2YR-NUZU].

30. *See* Petition for Writ of Certiorari at 14–18, United States v. Microsoft, No. 17-2-01 (U.S. June 23, 2017) (making a forceful argument that the Second Circuit erred in defining the focus of the relevant statute as being about protecting privacy); Petition for Rehearing and Rehearing En Banc at 11–17, Microsoft v. United States, No. 14-2985 (2d Cir. Oct. 13, 2016) [hereinafter Petition for Rehearing] (same).

31. *See, e.g.*, Peter Swire & DeBrae Kennedy-Mayo, *How Both the EU and the U.S. are "Stricter" Than Each Other for the Privacy of Government Requests for Information*, 66 EMORY L.J. 617, 617–23, 642–48 (2017).

32. The one way the ruling promotes privacy is by placing numerous roadblocks in the way of the government accessing data, thereby leading to a reduction in what law enforcement can obtain. But it does so based on the arbitrary fact of where the data is located, not on any normative determination that the kind of data sought should be protected. Were the data physically in the United States, just about everyone would agree that it could be lawfully obtained pursuant to a warrant based on probable cause, and that there would be no privacy violation in doing so—assuming there were an accurate and legitimate finding of probable cause.

the U.S.-based companies that control it, the ruling requires law enforcement to make a diplomatic request for sought-after data employing the mutual legal assistance process. But the United States has mutual legal assistance treaties ("MLATs") with only about one-third of the world's countries.[33] In some cases, the sought-after data may be held in a country with which the United States does not have an MLAT in place and has no other workable means of accessing the data. Moreover, even when there is an MLAT in place, the lengthy response times mean that even if there is the possibility of accessing the sought-after data, it may not be provided in time for it to be useful.[34]

Of particular concern, in some situations there is *no* country that has jurisdiction to access the sought-after data. Google's systems, for example, are (as of the time of this writing) designed so that only its U.S.-based team can access sought-after data. Let's assume that U.S. law enforcement serves a warrant on Google for a certain email account. If some or all of the data is outside the United States, Google cannot lawfully respond according to the Second Circuit ruling.[35] Yet, if the data is located outside the United States, the relevant foreign government does not have jurisdiction over the *people* who can access the data, since all such personnel are located in the United States. As a result, there may not be any country with jurisdiction to compel production of sought-after data, even in the investigation of serious crimes.[36]

In recognition of this reality, numerous district and magistrate judges, sitting across multiple districts, have disagreed with the Second Circuit's ruling and come out the other way in cases involving Google and Yahoo!.[37] These lower courts have ordered Google and Yahoo! to

---

33. *See Treaties, Agreements, and Asset Sharing*, U.S. DEP'T ST., https://www.state.gov/j/inl/rls/nrcrpt/2014/vol2/222469.htm (last visited Oct. 18, 2017) [https://perma.cc/5YX6-J5ME] (listing countries with which the United States currently has an MLAT in place).

34. *See, e.g.*, Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L SECURITY J. (Jan. 28, 2015, 1:05 PM), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age [https://perma.cc/ZML9-KB7B] (noting that it often takes months if not years for foreign governments to respond to MLAT requests).

35. Microsoft Ireland, 829 F.3d 197, 220–21 (2d Cir. 2016); *see also* Petition for Rehearing, *supra* note 30, at 17–19 (making this point).

36. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 719 (E.D. Pa. 2017) (disagreeing with the Second Circuit, ordering Google to disclose extraterritorially located data, and relying in part on concerns that there would be no alternative means for the government to access that data); *see also* Petition for Rehearing, *supra* note 30, at 17–19 (emphasizing the inability to access certain data from Google).

37. *See, e.g.*, *In re* Search Warrant to Google, Inc., No. 17-mj-532, slip op. at 23 (N.D. Ala. Sept. 1, 2017); *In re* Search Warrant No. 16-960-M-1 to Google, No. 16-960, 2017 WL 3535037, at *11 (E.D. Pa. Aug. 17, 2017), *aff'g* 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017); *In re* Search of Content Stored at Premises Controlled by Google Inc., No. 16-mc-80263, 2017 WL 3478809, at *5

disclose communications content located outside the United States in response to warrants based on probable cause. Lower court judges have disagreed with the Second Circuit both about the relevant focus of the statute (concluding that it is about disclosure, not privacy) and about the locus of any privacy violation (in the United States when turned over to law enforcement, not where it is accessed).[38] Various judges have also emphasized the practical problems created, particularly in situations where data is constantly being moved around and there is no stable single location.[39]

In October 2017, the U.S. Supreme Court agreed to hear the *Microsoft Ireland* case.[40] The fact that the Supreme Court took the case even in the absence of a circuit split highlights its perceived importance. But there is reason to hope, however, that Congress steps in and ultimately moots the case before the Court.[41] Specifically, Congress should clarify that the warrant authority under the ECPA is not limited based on the location of the data. Yet, it should also ensure respect for the countervailing interests of foreign governments in controlling access to their own citizens' and residents' data—much as the United States would (and should) demand if foreign governments sought to access U.S. residents' and citizens' data.[42] I return to this issue in Part III.

(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, No. 16-mj-2197, 2017 WL 3263351, at *9 (C.D. Cal. July 13, 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). Decisions have noted that the location of data at any given moment was the consequence of an algorithmic decision untethered to user location. Decisions have also highlighted the impossibility of lawfully accessing certain information via diplomatic channels, given the way Google has designed its system. *See, e.g.*, *In re Search Warrant*, 232 F. Supp. 3d at 725 (noting that "if the court were to adopt Google's interpretation of the Microsoft decision and apply such a rationale to the case at bar, it would be impossible for the Government to obtain the sought-after user data through existing MLAT channels").

38. *See supra* note 37.

39. *See, e.g.*, *In re Search of Content*, 2017 WL 3478809, at *4; *In re Search Warrant No. 16-960-M-01*, 232 F. Supp. 3d at 724–25.

40. United States v. Microsoft Corp., No. 17-2, 2017 WL 2869958, at *1 (U.S. Oct. 16, 2017).

41. *See* Jennifer Daskal, *There's No Good Decision in the* Microsoft Ireland *Case*, N.Y. TIMES (Oct. 18, 2017), https://www.nytimes.com/2017/10/18/opinion/data-abroad-privacy-court.html [https://perma.cc/TH47-JMZN]; Jennifer Daskal, *Whose Law Governs in a Borderless World?*, NAT'L CONST. CTR. (May 9, 2017), https://constitutioncenter.org/blog/whose-law-governs-in-a-borderless-world [https://perma.cc/CE86-L9M7].

42. In fact, even the Second Circuit Judge who authored the opinion has urged Congress to step in. *See In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 855 F.3d 53, 55 (2d Cir. 2017) ("It is overdue for a congressional revision that

2. The Belgian Approach: Give Us Everything

The approach taken by the Belgian courts in two recent cases—one involving Yahoo! and a second involving Skype—marks a sharp contrast to the location-driven approach taken by the Second Circuit in the *Microsoft Ireland* case. It too, is troubling, albeit for different reasons.

The dispute with Yahoo! began in November 2007 when Belgian authorities sought IP and email addresses as well as other information that would assist in the identification of particular individuals in a computer fraud case. Yahoo! refused to comply, and the company was prosecuted, convicted, and fined fifty-five thousand Euros in damages, plus an additional ten thousand Euros for each day it failed to provide the sought-after data.[43] Yahoo! appealed, making three key arguments. First, Yahoo! argued it was neither an electronic communication network nor a provider of electronic communication services and thus that it was outside the scope of the applicable Belgian statute. Second, Yahoo! argued that, as a U.S. company that lacked any presence in Belgium, the applicable Belgian statute did not apply. And third, Yahoo! argued that even if it were covered by the statute, the production order constituted an impermissible extraterritorial application of Belgian enforcement jurisdiction.[44]

After a lengthy set of appeals, the Belgian Supreme Court rejected all of Yahoo!'s arguments and upheld the conviction. Specifically, it ruled that Yahoo! was a provider of electronic communication services that fell within the relevant statute. It further concluded that the statutory disclosure obligations cover "any operator or provider that actively aims its economic activities on [Belgian]

---

would continue to protect privacy but would more effectively balance concerns of international comity with law enforcement needs and service provider obligations in the global context in which this case arose."); *see also In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 222 (2d Cir. 2017) (Lynch, J., concurring) (writing separately, in part, to "emphasize the need for congressional action to revise a badly outdated statute").

43. *See* 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), http://sas-space.sas.ac.uk/5720/1/2138-3141-1-SM.pdf [https://perma.cc/QG59-GAHW]; Hof van Cassatie [Cass.] [Court of Cassation], Dec. 1, 2015, Nr. P.13.2082.N (Belg.) (rejecting appeal by Yahoo!), *translated in* 13 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 156 (2016), http://journals.sas.ac.uk/deeslr/article/viewFile/2310/2261 [https://perma.cc/A2ZM-KVZC]; Paul de Hert & Monika Kopcheva, *International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case*, 27 COMPUTER L. & SECURITY REV. 291, 292 (2011).

44. Procureur-Général v. Yahoo! Inc., Hof van Cassatie [Cass.] [Court of Cassation], Jan. 18, 2011, Nr. P.10.1347.N (Belg.), *translated in* 8 DIGITAL EVIDENCE & ELECTRONIC SIGNATURE L. REV. 216, 216–18 (2011), http://journals.sas.ac.uk/deeslr/article/view/1978/1915 [https://perma.cc/8FT2-DZKU].

consumers," even if the company does not have a physical presence in Belgium.[45]

The Belgian Court also reasoned its way around the extraterritorial enforcement concerns:

> This measure does not require the presence abroad of Belgian police officers or magistrates or any persons acting on their behalf. Neither does the measure require any material action to be taken abroad. It is therefore a coercive measure with limited extent, the execution of which *does not require any intervention* outside the Belgian territory.[46]

In contrast to the approach taken by the *Microsoft Ireland* case, the Belgian court held that territoriality is determined based on where the data is accessed and received, not where it is located.

While far reaching, the Yahoo! case was arguably limited by its facts; specifically, it involved a request for subscriber information only.[47] Subscriber information is generally deemed less revealing of personal information than communications content. It is, as a general matter, subject to fewer substantive and procedural protections.[48] For similar reasons, State A's unilateral demands for subscriber information located in or held by a provider in State B are generally deemed less of an intrusion of sovereign interests than State A's equivalent demands for communications content.

But in a subsequent case against Skype, the Belgian courts extended the decision to cover communications content as well. Belgian prosecutors issued an order to disclose both noncontent *and* content data regarding communications between two Belgian residents, as well as technical assistance from Skype in obtaining these communications.[49] Although Skype provided basic registration information, it asserted that it did not retain or have access to the content of communications and other information that Belgian authorities sought. Skype further argued that as a company

---

45. *Id.*

46. *Id.* ¶ 6 (emphasis added). The court also focused on the fact that the request was made in pursuit of the investigation of an offense that fell within the scope of Belgian criminal jurisdiction and was aimed at identification data only.

47. *See* Hert & Kopcheva, *supra* note 43, at 295.

48. This, however, is a premise that is increasingly coming under attack. *See, e.g.*, Danielle Citron & David Gray, *The Right to Quantitative Privacy*, 98 MINN. L. REV. 62, 140–41 (2013); Dahlia Lithwick & Steve Vladeck, *Taking the "Meh" Out of Metadata*, SLATE (Nov. 22, 2013, 12:07 PM), http://www.slate.com/articles/news_and_politics/jurisprudence/2013/11/nsa_and_metadata_how_the_government_can_spy_on_your_health_political_beliefs.html [https://perma.cc/GMY8-XEFZ].

49. Procureur-Général v. Skype, Correctionele Rechtbanken [Corr.] [Criminal Tribunal] Antwerp, Division Mechelen, Oct. 27, 2016, No. ME20.4.1 105151-12, ¶¶ 1.2–1.5 (Belg.).

headquartered in Luxembourg, any such request for communications content should be directed to the Luxembourg government, not Skype.[50]

Skype lost in both the lower court and on an initial appeal.[51] The lower court concluded that, even though Skype was based in Luxembourg, it had subjected itself to Belgian jurisdiction by "actively participating in the economic life in Belgium" and offering services there.[52] Relying on the Belgian Supreme Court's decision in Yahoo!, the lower court judge defined the relevant enforcement action as territorial, not extraterritorial.[53] The court emphasized that, as in the Yahoo! case, no Belgian investigators would be entering another country, and the sought-after information would be turned over in Belgium. The court also dismissed concerns about a potential conflict with Luxembourg law or infringement of Luxembourg's sovereignty: "A possible conflict with Luxembourg law is not relevant here, given the fact that Skype had to provide its technical cooperation on Belgian territory and not in Luxembourg."[54] The appellate court fully agreed, adopting and referring to the lower court's reasoning throughout its opinion.[55]

The Skype and Yahoo! cases raise additional considerations not presented by the *Microsoft Ireland* case. In the *Microsoft Ireland* case, U.S. law enforcement had clear jurisdiction over Microsoft; Microsoft is based and headquartered in Redmond, Washington. In contrast, neither Yahoo! nor Skype has any physical presence in Belgium. The Belgian courts concluded nonetheless that jurisdiction existed over a company that offered services in and "participated in the economic life" in Belgium, even if it was not physically present.[56] A company that advertises in and provides tailored technical assistance to the state's residents, as Skype and Yahoo! did, is subject to Belgium's jurisdiction under this approach.[57]

---

50. *Id.* ¶ 1.9. There was also a separate argument as to whether Skype constituted either an "operator or a telecommunications network" or "provider of a telecommunication services" subject to the disclosure obligations. Skype claimed it did not, but the court concluded it did. *Id.* ¶¶ 5.1.2, 5.2.

51. *See* Openbaar Ministerie v. Skype Communications SARL, Hof van Beroep [HvB] [Court of Appeal] Antwerp, Nov. 15, 2017, 2016/CO/1006 (Belg.); *see also Procureur-Général v. Skype.*

52. In reaching this conclusion, the court emphasized that the company made its software available for use on the Belgian territory, maintained a website and user manuals that could be accessed in Dutch, and provided assistance and support in Dutch to users that encountered software troubles. *Procureur-Général v. Skype*, ¶ 5.3.4.

53. *Id.* ¶ 5.3.2–5.3.35.

54. *Id.* ¶ 5.5.3.

55. *Openbaar Ministerie v. Skype*, ¶¶ 5.1.1.4., 5.1.2.2.

56. *Id.* ¶ 5.5.5.

57. Of course, if a provider lacks any presence of physical property in the territory, the requesting government may not have any means of enforcing compliance, other than perhaps by shutting down the service or otherwise blocking residents' access to its products. *See* Jack L. Goldsmith, *Against Cyberanarchy*, 65 U. CHI. L. REV. 1199, 1216–21 (1998) (emphasizing the

The Belgian courts also endorsed an entirely new and potentially infinitely expansive ground for determining territoriality—based on where data is *received*, even if the relevant provider is not physically located in the receiving state's territory. In the *Microsoft Ireland* case, the dispute was whether territoriality is determined based on where the *data* is located (Ireland) or where the *provider* is located and accesses the data (the United States). In the Yahoo! case, by contrast, both the data *and* the provider were located extraterritorially. The Belgian Supreme Court nonetheless concluded that the production order was territorial because the sought-after data was received within the requesting state's territorial boundaries. It is an approach that essentially makes any production order territorial, regardless of other considerations that might apply. The only relevant question becomes whether there is a domestic, lawful basis to compel.

Such a reformulation of the definition of "territorial" serves Belgian domestic law enforcement interests. Yet it has a number of concerning implications. If applied broadly, such an approach would mean that states could assert access to any data of interest, without regard to countervailing interests of other states. If employed by states with poor human rights records, it would yield a reduction of privacy rights and the facilitation of other abuses based on how accessed data is used. It also means that users would—absent the adoption of some sort of globally applicable notice requirement—have no way to determine which jurisdiction is accessing their data and under which rules, with significant consequences for, among other things, the possibility of either redress or democratic accountability. Such an approach thus fails to respect the sometimes legitimate sovereign interest in regulating access to data of a state's own nationals and residents. And as a practical matter, it runs up against blocking provisions enacted by a number of jurisdictions, including the United States and most European countries—an issue I turn to now.

3. Blocking Provisions

Blocking provisions prohibit locally based providers from disclosing data to foreign law enforcement officials, even if requested pursuant to lawful process by the foreign jurisdiction. The same statute that is at issue in the *Microsoft Ireland* case, for example, also prohibits U.S.-based providers from directly disclosing U.S.-held stored

practical limits of enforcement jurisdiction). In both the Yahoo! and Skype cases, the companies voluntarily submitted themselves to the relevant court's jurisdiction.

communications content to foreign-based providers.[58] Any foreign law enforcement entity that seeks access to such data must make a mutual legal assistance request to the United States—and ultimately obtain a U.S. warrant based on the U.S. standard of probable cause.[59] This is so regardless of the location of the target of the investigation or the criminal activity that is being investigated. It is the source of an increasing amount of frustration on behalf of foreign governments, particularly when foreign governments are seeking data in the investigation of local crime and the only U.S. nexus to the case is that the sought-after data happens to be held by a U.S.-based provider within U.S. territorial boundaries.[60] Such blocking provisions also create a direct conflict of laws if and when a foreign government—such as Belgium—compels production of data that another country—such as the U.S.—prohibits a provider from producing. This kind of conflict is not just hypothetical. In January 2015, a Microsoft employee was arrested in Brazil for failing to comply with Brazilian disclosure requirements, even though U.S. law prohibited him from doing so.[61]

Many European countries have similar, and even broader, blocking provisions than those in place in the United States—covering noncontent data as well as communications content.[62] The newly enacted General Data Protection Regulation, for example, scheduled to

---

58. The Stored Communications Act ("SCA") prohibits providers from turning over the content of communications, except in a limited number of situations. *See* 18 U.S.C. §§ 2702–2703(a) (2012). While a "governmental entity" may compel such production, pursuant to a lawfully issued warrant, "governmental entity" is defined as "a department or agency of the United States or any State or political subdivision thereof." 18 U.S.C. § 2711(4). Thus, foreign governments do not qualify.

59. *See* RICHARD A. CLARKE ET AL., LIBERTY AND SECURITY IN A CHANGING WORLD: REPORT AND RECOMMENDATIONS OF THE PRESIDENT'S REVIEW GROUP ON INTELLIGENCE AND COMMUNICATIONS TECHNOLOGIES 227–28 (2013) (noting that it takes an average of ten months to process these MLAT requests).

60. The scope of the prohibitions on disclosure is not spelled out in the statute. As a result, the statute does not specify whether the prohibition governs all U.S.-based corporations, all U.S.-held data, or both. *See* 18 U.S.C.A § 2703 (West 2009). Under the reasoning of the Second Circuit *Microsoft Ireland* decision, the prohibition would apply to U.S.-held data only. In the wake of that decision, the Department of Justice reportedly has been telling requesting governments that they first must ascertain that the sought-after communications content is in the United States before making a mutual legal assistance request for such data; previously, the Department of Justice would accept such a request directed at data held by U.S.-based providers without regard to location. Interview with Eur. Comm'n representative (Jan. 25, 2017) (notes on file with author).

61. *See, e.g.*, Brad Smith, *In the Cloud We Trust*, MICROSOFT STORIES, https://news.microsoft.com/stories/inthecloudwetrust/ (last visited Oct. 18, 2017) [https://perma.cc/RGQ6-P8C6] (describing the 2015 arrest of a Microsoft employee by Brazilian authorities for failing to turn over data that he was prohibited from disclosing under U.S. law).

62. *See* EUR. COMM'N, NON-PAPER: PROGRESS REPORT FOLLOWING THE CONCLUSIONS OF THE COUNCIL OF THE EUROPEAN UNION ON IMPROVING CRIMINAL JUSTICE IN CYBERSPACE 6 (Dec. 2, 2016), http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf [https://perma.cc/9GME-9L5Z] [hereinafter EUR. COMM'N REPORT].

go into effect in May 2018, prohibits the transfer of the personal data of EU residents outside the EU unless pursuant to specific exemptions, such as an explicit international agreement.[63] But there is currently no explicit legal basis for providers to turn over EU subjects' data to foreign law enforcement officials outside the EU, and as a result some have claimed that they are presumptively barred from doing so.[64]

Such blocking provisions are based on the presumption that the sovereign interests in data are coterminous with its location—and thus governments can and should set the rules governing foreign government access to data held by locally based providers within their territorial jurisdictions. But as we saw in the discussion of the *Microsoft Ireland* case, this is a misguided assumption. The location of data is fluid, changeable, and changing, and as a result is often mismatched with the key security, privacy, economic, and other sovereign interests at stake. Why, after all, should the United States or any other nation demand that a foreign nation go through the diplomatic process to access the data of a local target in a local crime investigation simply because the data of interest happens to be stored within the United States' territorial jurisdiction? Such a rule reflects a mismatch between technology, law, and the underlying interests the law is meant to serve.

That said, for many privacy advocates, these blocking provisions, at least as employed by the United States, are things to be celebrated. After all, the United States' warrant requirement imposes relatively robust substantive and procedural privacy protections, as compared with those employed by many other nations around the world.[65] Moreover, the Department of Justice reviews each foreign government request for communications content as part of the mutual

63. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016, art. 48, 2016 O.J. (L 119) 1 [hereinafter GDPR].

64. *See, e.g.*, CEG REPORT, *supra* note 7, at 16 (noting the legal basis for the so-called "asymmetric" sharing of personal identification information across borders—i.e., from governments to service providers as part of a request for additional information and from service providers to governments in response—is not so clearly established). There are, however, agreements that explicitly permit the law-enforcement-to-law-enforcement sharing of data. *See* Agreement Between the United States of America and the European Union on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, E.U.-U.S., at 4, Aug. 9, 2015, http://ec.europa.eu/justice/data-protection/files/dp-umbrella-agreement_en.pdf [https://perma.cc/9887-7M24]; Press Release, Eur. Comm'n, Questions and Answers on the EU-U.S. Data Protection "Umbrella Agreement" (Dec. 1, 2016), http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm [https://perma.cc/JK3W-ESXU] (discussing the intent to facilitate data transfer between the EU and United States "for the purpose of preventing, investigating, detecting or prosecuting criminal offenses . . . in the framework of police cooperation and judicial cooperation in criminal matters").

65. *See, e.g.*, Greg Nojeim & Ross Schulman, *Foreign Governments, Tech Companies, and Your Data: A Response to Jennifer Daskal & Andrew Woods*, JUST SECURITY (Aug. 30, 2016, 4:05 PM), https://www.justsecurity.org/32529/foreign-governments-tech-companies-data-response-jennifer-daskal-andrew-woods/ [https://perma.cc/GRV4-EG8A].

legal assistance process, including an assessment as to the implications for free speech—thus ensuring that data is not being sought to prosecute individuals for engaging in what would be protected speech under the First Amendment. The application of U.S. rules and standards thus enhances both privacy and speech rights in specific cases. EU countries similarly can rely on their own blocking provisions to limit access by other repressive regimes.

But what this analysis neglects is the long-term effect of these restrictions. Frustrated governments will, if sufficiently sophisticated, find ways around the restrictions if the stakes are sufficiently high. These work-arounds include costly data localization requirements, pursuant to which providers are required to cache copies of data locally, thus facilitating access by local governments; the use of alternative, surreptitious means of accessing sought-after data; and increasing assertions of extraterritorial jurisdiction that ignore the existence of countervailing blocking provisions and put providers in the middle of a conflict of laws problem, forcing them to choose which law to adhere to and which to violate.[66]

4. Nascent Reform Efforts: The EU, U.S., and Efforts at Harmonization

Increased frustration caused by the inability to access data needed for criminal investigations in a timely matter and uncertainty over the rules that apply are yielding calls for reform within the EU, the United States, and in coordinated efforts between the United States and the U.K.

a. Council of Europe: Updates to the Budapest Convention

The Budapest Convention's Cloud Evidence Group, established in 2014 by the state parties to the Budapest Convention, has long focused on the difficulties in accessing data across borders and urged updates to better account for law enforcement needs in accessing data

66. *See, e.g.*, Peter Swire, *Why Cross-Border Government Requests for Data Will Keep Becoming More Important*, LAWFARE BLOG (May 23, 2017, 10:00 AM), https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important [https://perma.cc/XNP6-ZGFM] (making the point that if law enforcement is unable to make workable requests for data, it will face increased pressure to either try to break encryption or remotely hack into a device of interest); Andrew Keane Woods, *Lessons from the Mutual Legal Assistance Reform Effort*, LAWFARE BLOG (May 22, 2017, 1:00 PM), https://www.lawfareblog.com/lessons-mutual-legal-assistance-reform-effort [https://perma.cc/9J94-TBKM] (arguing that the mutual legal assistance debate is tied to the encryption debate).

in the cloud.[67] In June 2017, the group announced the initiation of a two-year-long effort to draft a new protocol to the Convention that would, if adopted, facilitate law enforcement access to data in foreign, multiple, and unknown jurisdictions.[68]

Recent efforts also have led to a newly adopted guidance note to accompany Article 18 of the Convention, albeit limited to subscriber information only.[69] While not binding, the guidance note highlights an evolution in thinking as well as continued stickiness of the linkage between data location and sovereign interest in control.

Article 18 includes two parts. It requires state parties to establish mechanisms by which law enforcement officials can order "a *person* in its territory to submit specified computer data in that person's possession or control."[70] This provision applies to both content and noncontent data. It also requires that state parties establish mechanisms by which law enforcement officials can order a service provider "offering its services in the territory of the Party" to turn over subscriber information in that service provider's possession or control.[71] The provision itself is silent as to whether or not there are any territorial limits on what can be produced.

The recently adopted guidance note seeks to clarify the territorial reach of these two provisions as applied to compelled disclosure orders directed at service providers—but for subscriber information only.[72] First, it makes explicit that providers should be required to produce all subscriber information within their possession or control, regardless of the location of the data. In so doing, it explicitly rejects a data location–driven approach to disclosure obligations, at least with respect to subscriber information.[73]

---

67. AD-HOC SUBGROUP ON TRANSBORDER ACCESS & JURISDICTION, COUNCIL OF EUR., TRANSBORDER ACCESS TO DATA AND JURISDICTION: OPTIONS FOR FURTHER ACTION BY THE T-CY 7 (Dec. 3, 2014), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016802e726e [https://perma.cc/YH3K-ETPF] [hereinafter TRANSBORDER ACCESS TO DATA AND JURISDICTION].

68. *See* Cybercrime Convention Comm. Proposal, *supra* note 9; *Cybercrime*, *supra* note 9.

69. Cybercrime Convention Comm. Guidance, *supra* note 9, at 9 (noting that the guidance note "represents the common understanding of the Parties as to the scope and elements of Article 18 Budapest Convention *with respect to the production of subscriber information*" (emphasis added)).

70. Convention on Cybercrime, Nov. 23, 2001, T.I.A.S. No. 13,174, 10 E.T.S. No. 185, http://www.europarl.europa.eu/meetdocs/2014_2019/documents/libe/dv/7_conv_budapest_/7_conv_budapest_en.pdf [https://perma.cc/AH8T-BMJ6].

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

72. *See* Cybercrime Convention Comm. Guidance, *supra* note 9, at 3.

73. In the words of the guidance note, "Legal regimes increasingly recognize, both in the criminal justice sphere and in the privacy and data protection sphere, that the location of the data is not the determining factor for establishing jurisdiction." *Id.* at 7.

Second, it clarifies the state's jurisdictional reach over extraterritorially located providers, advocating a rule with broad jurisdictional reach. Specifically, it covers any provider that enables persons in the territory to use its service and orients its activities toward those persons (e.g., providers that engage in advertising in the relevant jurisdiction, even if they lack a physical presence there).[74] This is akin to the broad jurisdictional hook adopted by the Belgian courts in the Yahoo! and Skype cases, although limited to situations in which the government is seeking subscriber information only.

Such a broad jurisdictional hook seems, at first blush, to reject the view that states' access to sought-after data depends either on where it happens to be held or where the provider happens to be located. Rather, what matters is that the provider offers services in the jurisdiction and that there is a lawful domestic basis to access the data by the requesting state—that the information is relevant to a legitimate domestic investigation and that the relevant procedural and substantive criteria in the requesting state have been met.[75]

But on further evaluation, the note is much less far reaching than it initially appears. At the same time that the note endorses the authority of state parties to compel the production of subscriber information from extraterritorially located service providers, it also supports the continued right of states to block such requests. In the note's words, "[a]greement to this Guidance Note does not entail consent to the extraterritorial service or enforcement of a domestic production order issued by another State."[76] In other words, the guidance note endorses states' authority to reach service providers beyond their borders, yet refuses to disclaim government efforts to block such foreign government reach.

Moreover, the unwillingness and inability of the parties to the EU Cybercrime Committee to endorse—even in this tepid way—the

---

74. *See* COUNCIL OF EUR., EXPLANATORY REPORT TO THE CONVENTION ON CYBERCRIME 29 (2001), https://rm.coe.int/16800cce5b [https://perma.cc/K8FC-37VT].

75. Depending on how interpreted and applied, this approach could require several U.S.-based providers to change their current practices. U.S.-based providers can, as a matter of law, provide any subscriber information to requesting foreign law enforcement (the blocking provisions only apply to content). But several providers have in place internal rules that preclude them from providing subscriber information about customers located outside the jurisdiction of the requesting state. *See* CEG REPORT, *supra* note 7, at 27 (noting concern about "self-made rules barring disclosures when an IP address resolves to a country other than the requesting country"). This guidance note, however, includes no such limitation based on location of the target.

76. Cybercrime Convention Comm. Guidance, *supra* note 9, at 6. The guidance note also states that "[t]he service and enforceability of domestic production orders against providers established outside the territory of a Party raises further issues which cannot be fully addressed in a Guidance Note. Some Parties may require that subscriber information be requested through mutual legal assistance." *Id.* at 1.

authority of foreign governments to compel the production of communications *content* located or held by a subscriber outside their borders is notable, especially given that the category of "person" in the first part of Article 18 covers service providers and is not, on its face, limited to subscriber information. This reflects at least three considerations: first, that communications content is often deemed more sensitive, and thus deserving of stronger protections than subscriber information;[77] second, that states have, as a result, a greater interest in limiting access to such data; and third, the stickiness of the linkage between sovereignty and territory, irrespective of other normative and practical considerations. I return to these issues in Section II.B.

b. The EU Reform Effort

Parallel to the Council of Europe's efforts, the EU is working to develop its own response to the jurisdictional challenges. This is made difficult by the wide diversity of approaches to the jurisdictional questions even amongst EU member states. For some EU members, jurisdiction turns on the "main seat of the service provider"; for some "the place where services are offered"; and for others "the place where data is stored"; a recent European Commission report also noted "a combination of [unspecified] alternatives" as well.[78] As a recent European Commission report put it, "[t]he use of different approaches creates legal uncertainty for authorities issuing requests, as well as for service providers to which the requests are directed."[79] The report further warns that "the legal uncertainty may also interfere with rights of the persons to which the requested evidence relates, including their right to privacy.[80]

In response, the European Commission has launched an initiative designed to "address obstacles in cross-border access to electronic evidence in criminal investigations."[81] The project aims at facilitating cross-border access to data amongst EU members. It also seeks to address the need for access to data outside the EU, in particular data held by the United States.[82]

---

77. *See supra* note 48.

78. *See* EUR. COMM'N REPORT, *supra* note 62, at 5.

79. *Id.* at 13.

80. *Id.*

81. *Improving Cross-Border Access to Evidence in Electronic Matters*, EUR. COMMISSION 3 (Mar. 8, 2017), https://ec.europa.eu/info/law/better-regulation/initiatives/ares-2017-3896097_en [https://perma.cc/S788-D6S6] [hereinafter Inception Impact Assessment].

82. *Id.* at 2.

Meanwhile, the European Investigative Order ("EIO") offers a way to facilitate improved government-to-government cooperation via a system of mutual recognition. An EIO is a judicial decision issuing or approving a request for evidence from one state (the "requesting" state) to another (the "executing" state).[83] With a few specified exceptions, the executing state is required to give effect to an EIO as if they had been issued by the state's own domestic authority—thus streamlining the process of government review and expediting response times.[84]

But while streamlined, the executing country still has up to thirty days to determine whether to recognize the EIO and another ninety days to carry out the requested investigative measure. In a fast-moving investigation, this is a very long time. Moreover, the Directive establishing the EIO presumes that participating states will know where to direct the request. It thus provides a mechanism for improved state-to-state cooperation when there is consensus about who has territorial control, but it does not resolve the first order questions as to the basic source of territorial control. Is it the location of the data? The provider? The target? The crime? Or some combination thereof? Until there is some additional clarity as to those questions, participating states are likely to continue to clash over the basic question of whether an EIO is even needed, or whether they can simply assert territorial control—as envisioned by the newly adopted guidance note to Article 18 of the Budapest Convention, albeit with respect to subscriber information only, and exemplified by the Belgian approach in the Yahoo! and Skype cases.

c. U.S. Legislative Proposals and the U.S.-U.K. Agreement

Because of the dominance of U.S.-based service providers, foreign governments regularly find themselves seeking data subject to U.S. jurisdiction. This also means that U.S. blocking provisions that prohibit U.S.-based companies from directly disclosing communications to foreign law enforcement is a particular source of frustration for foreign governments. In response, the United States and United Kingdom have negotiated a draft agreement that would lift some of these restrictions and permit U.K. law enforcement to directly access

83. Directive 2014/41/EU, of the European Parliament and of the Council of 3 April 2014 Regarding the European Investigation Order in Criminal Matters, 2014 O.J. (L 130) 1, 6–7 [hereinafter Investigation Directive] (discussion of Article 1).

84. *Id.* at 2.

communications content held by U.S.-based providers in certain specified circumstances.[85]

While the actual text of the draft agreement has not yet been released, the basic contours have been spelled out in a variety of public statements—and in the outlines of draft legislation needed to implement such an agreement.[86] It would permit the U.K. to directly compel the production of communications content of non-U.S. citizens located outside the United States, but only if specified criteria are met. Among other requirements, the requests would have to be particularized, subject to judicial review, and subject to minimization requirements to protect against the retention and dissemination of nonrelevant information.[87] If the U.K. law enforcement officials sought the communications content of a U.S. resident or citizen (wherever located), it would still need to employ the mutual legal assistance process and ultimately obtain, via a U.S. prosecutor, a U.S.-issued warrant based on probable cause.

As already indicated, however, the draft agreement cannot be implemented unless and until the U.S. Congress passes legislation to amend the statutory bar.[88] Draft legislation submitted by the Department of Justice to Congress in 2016, and again in 2017, would do just that.[89] It would explicitly permit the United States to enter into the kind of executive agreements contemplated with the United

85. *See, e.g.*, *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests: Hearing Before the H. Comm. on the Judiciary*, 114th Cong. 9–15 (2016) [hereinafter *International Conflicts Hearing*] (statement of David Bitkower, Principal Deputy Assistant Att'y Gen., Criminal Division, Department of Justice); Nakashima & Peterson, *supra* note 10.

86. *See* Letter from Samuel R. Ramer, Assistant Attorney Gen., to Paul Ryan, Speaker of the U.S. House of Representatives (May 24, 2017), https://judiciary.house.gov/wp-content/uploads/2017/06/Downing-Testimony.pdf [https://perma.cc/Q7JM-4ARP] [hereinafter Letter to Ryan]; *International Conflicts Hearing*, *supra* note 85 (statement of David Bitkower conveying a framework in which the United States may disclose data directly to the United Kingdom and receive reciprocal access to data stored in the United Kingdom); Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President of the U.S. Senate (July 15, 2015), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf [https://perma.cc/UX34-6UWS] [hereinafter Letter to Biden] (conveying proposed legislation and a section-by-section analysis).

87. Letter to Ryan, *supra* note 86 (setting out these requirements as a matter of statute); Letter to Biden, *supra* note 86.

88. *See* Letter to Ryan, *supra* note 86; Letter to Biden, *supra* note 86.

89. *International Conflicts Hearing*, *supra* note 85 (statement of Jennifer Daskal, Assistant Professor, American University Washington College of Law); Letter to Ryan, *supra* note 86; Letter to Biden, *supra* note 86; *see also* Jennifer Daskal & Andrew K. Woods, *Congress Should Embrace the DOJ's Cross-Border Fix*, JUST SECURITY (Aug. 1, 2016, 8:03 AM), https://www.justsecurity.org/32213/congress-embrace-dojs-cross-border-data-fix/ [https://perma.cc/GUP7-WU8C]; David Kris, *U.S. Government Presents Draft Legislation for Cross-Border Data Requests*, LAWFARE (July 16, 2016, 8:07 AM), https://www.lawfareblog.com/us-government-presents-draft-legislation-cross-border-data-requests [https://perma.cc/P4FL-TE2B].

Kingdom so long as certain conditions are met. First, the Attorney General and Secretary of State would need to certify that the partner nation demonstrates basic respect for the rule of law. Second, it specifies a number of requirements that each foreign government request for data must meet—including, among other things, that the requests be targeted, particularized, time-limited, and reviewed or overseen by a court or other independent entity. Third, it prohibits foreign governments from directly accessing the data of U.S. citizens and other persons living in the United States; the foreign government would still need to employ the mutual legal assistance process for those requests. And fourth, it requires that the partner state take steps to protect against the retention and dissemination of information about U.S. citizens and residents, and comply with various auditing requirements, transparency, and other accountability mechanisms.

The approach is interesting for two key reasons. First, it reflects a shift in focus from location of data or provider to location and nationality of the target as determinative of the rules that apply. Foreign partners can access non-U.S. citizen and resident data according to their own rules, but they need to abide by U.S. requirements when seeking the data of U.S. citizens and residents. This reflects the normative view that states have a legitimate interest in controlling access to their own citizens' and residents' data, but have much less of a justification in controlling access to the data of other extraterritorially located targets simply because of the fact that the sought-after data happens to be held locally.

Second, it makes clear that such requests are only legitimate if certain baseline standards are met. It thus uses the United States' leverage as the home to so much of the world's data to impose a set of baseline procedural and substantive standards that apply to law enforcement requests for data outside the United States. It lays out a minimum standard framework, saying only those requests that satisfy the basic due process requirements specified by the United States are eligible for this kind of expedited access. If successful, it could serve as a means of setting baseline standards in ways that enhance due process and privacy rights across borders. In fact, it seems that even the possibility of such a scheme has, in at least one instance, led to a modest raising of standards: recent amendments to U.K. surveillance laws require—for the first time ever—judicial review of compelled production orders for stored communication content. Informal discussions suggest that the U.K. Home Office was persuaded to support the judicial review provisions because, among other reasons,

they recognized they were needed in order for the United States to approve its draft agreement.[90]

B. Direct Government Access

The discussion so far has focused on compelled disclosure orders—pursuant to which the government seeks data held by third-party providers. A separate but related set of issues are raised by governmental efforts to directly access data or devices when the sought-after data or device is located across territorial borders. These issues were hotly debated in the leadup to recent amendments to Federal Rule of Criminal Procedure 41 in the United States, and have been the topic of conversation in the European Union and Council of Europe as well.

1. Rule 41 Amendments

On December 1, 2016, the newly amended Federal Rule of Criminal Procedure 41 went into effect.[91] For the first time, the U.S. criminal rules of procedure explicitly authorize remote search warrants and lift the jurisdictional limits that would otherwise apply. Specifically, the rules allow for a judge to issue a remote search warrant—what some have labeled a "lawful hacking" warrant—if the location of the target data or device is unknown and the location has been concealed due to technological means, such as the use of anonymization software like Tor.[92]

As several commentators have noted, the updated rule will almost inevitably result in judges inadvertently authorizing searches of

90. Interview with U.K. gov't officials, at U.K. Home Office (Nov. 12, 2016) (notes on file with author).

91. *See* FED. R. CRIM. P. 41(b)(6).

92. *Id.* At least one magistrate judge had under the prior version of the rule rejected such a warrant in these circumstances. The magistrate concluded that if the device were of an unknown location, it could potentially be outside his district—and thus outside his jurisdiction. *See In re* Warrant to Search a Target Comput. at Premises Unknown, 958 F. Supp. 2d 753, 756–61 (S.D. Tex. 2013). A handful of other courts have suppressed evidence obtained pursuant to remote search warrants for similar reasons. *See, e.g.*, United States v. Croghan, 209 F. Supp. 3d 1080 (S.D. Iowa 2016); *see also* Letter from Mythili Raman, Acting Assistant Attorney Gen., Criminal Div., U.S. Dep't of Justice, to Reena Raggi, Chair, Advisory Comm. on the Criminal Rules 2 (Sept. 18, 2013), http://www.justsecurity.org/wp-content/uploads/2014/09/Raman-letter-to-committee-.pdf [https://perma.cc/6Y6N-8JFXv] [hereinafter Letter from Raman to Raggi] (emphasizing that the circumstances "where investigators can identify the target computer, but not the district in which it is located . . . [are] occurring with greater frequency in recent years"); Leslie R. Caldwell, *Rule 41 Changes Ensure a Judge May Consider Warrants for Certain Remote Searches*, U.S. DEP'T JUST. (June 20, 2016), https://www.justice.gov/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches [https://perma.cc/ML7Y-Z55Y] (explaining need for rule change).

extraterritorially located data or devices;[93] after all, if the location of the data or device is unknown, it may very well be located across borders.[94] The U.S. government has acknowledged this possibility and stated that if the data or device ends up being extraterritorially located, the warrant will have no force (although the existence of the warrant will speak to the reasonableness of the search).[95] There is, after all, no Rule 41 authority to issue warrants for extraterritorially located property.

Some have suggested that such inadvertent accessing of data across borders will constitute a violation of foreign governments' sovereignty and thus international law. In the words of Professor Ahmed Ghappour, writing in the *Stanford Law Review*, "[t]he use of cross-border network investigative techniques undercuts the DOJ's democratic legitimacy to the extent it requires an interpretation of statutory investigative authority to extend overseas, . . . *in violation of customary international law*."[96]

Ghappour contrasts these remote hacking warrants with the kind of compelled disclosure orders at issue in the *Microsoft Ireland* case. In his view, a compelled disclosure order for data located extraterritorially does not violate international law, whereas remote searches conducted by law enforcement might. As he puts it: "Indirect collection of foreign-located evidence, by contrast, does not require the exercise of enforcement jurisdiction overseas. Instead, compelled disclosure orders impose an affirmative duty on third parties to disclose evidence in their possession or control . . . ."[97]

---

93. *See, e.g.*, Ghappour, *supra* note 13, at 1081 (calling the Rule 41 change the "largest expansion of extraterritorial law enforcement jurisdiction in FBI history").

94. The government is responding in part to the growing use of anonymization tools, the most predominant of which is Tor. But the vast majority of Tor users are foreign based, meaning that, in at least some situations, remote searches of Tor-users' devices will yield the search of a device located in a foreign territory. *See Top-10 Countries by Relay Users*, TOR METRICS, http://metrics.torproject.org/userstats-relay-table.html (last visited Oct. 20, 2017) [https://perma.cc/C7AP-5K8T] (estimating that about nineteen percent of Tor's daily users are based in the United States).

95. Letter from Raman to Raggi, *supra* note 92, at 5.

96. Ghappour, *supra* note 13, at 1126 (objecting, in part, to the process by which the rule change came about). Others have similarly claimed, albeit in different contexts, that remote intrusions that involve "the transmission of electrical impulses in a manner that change[s] (and d[oes] not simply observe) the physical *status quo* in a foreign computer system" violate the prohibition on extraterritorial law enforcement jurisdiction. *See* Craig Forcese, *The "Hacked" US Election: Is International Law Silent, Faced with the Clatter of Cyrillic Keyboards?*, JUST SECURITY (Dec. 16, 2016, 1:52 PM), https://www.justsecurity.org/35652/hacked-election-international-law-silent-faced-clatter-cyrillic-keyboards/ [https://perma.cc/649W-HRWR]. The copying of data involved in a Rule 41–authorized search would involve such "transmission of electronic impulses," even if it did not change the user's ability to access or manipulate the data. It would thus, under this test, constitute an impermissible exercise of law enforcement authority.

97. Ghappour, *supra* note 13, at 1103.

But more is needed to explain why this distinction between direct and indirect access is as salient as Ghappour has suggested, so long as the data is merely copied and not otherwise altered in both cases. There are, of course, important reasons to be concerned about the scope of lawful hacking orders. There is, for example, a reasonable likelihood that lawful hacking will yield access to a much broader amount of data than the targeted bit of information turned over pursuant to compelled disclosure orders. And lawful hacking, if not appropriately targeted, can sweep in the data of innocent users and/or lead to the triggering of other invasive surveillance techniques.[98] But assuming for the sake of argument that the data obtained is equivalent, it is hard to understand why the key sovereignty, security, and privacy interests would vary based on whether it is law enforcement agents or third-party providers accessing the data. In both cases, law enforcement agents in State A never set foot in State B's territory; the law enforcement agent and private party caretaker are similarly situated, at least in that respect.

To be clear, I am not saying that law enforcement should be given free rein to access data held in another state's jurisdiction. But what I am saying is this: to the extent such direct access raises concerns (which I accept it often does), the concerns seem to me due to something other than the fact that it is remote access by law enforcement, as opposed to remote access by a third party. Rather, the concerns are about *what* is accessed (and there *is* a real risk law enforcement access will not be sufficiently targeted), and the tools used to access it (given among other things the risk of network investigative techniques going awry), and not primarily about who is accessing the data.

It is also hard to understand why the *inadvertent* accessing of data in other jurisdictions, even by law enforcement, is necessarily a violation of sovereignty. To the contrary, informal conversations suggest that most governments, including the United States, appreciate if and when a foreign government inadvertently uncovers evidence about a local device or individual and discloses that information to the host country in a way that can then be used to make an arrest or otherwise shut down malicious activity.[99] It thus seems that any

98. Remote searches that involve the use of invasive network investigative techniques that, for example, threaten to spread malware throughout the system or involve the use of remote activation of a device's microphone or camera raise separate concerns; such intrusions are obviously more invasive. But even in these circumstances, it is not obvious that the *inadvertent* accessing of data or a device in a foreign government's jurisdiction would necessarily constitute a *sovereignty* violation (as opposed to other kinds of violations) if coupled with notice to the foreign government once the location of the device was discovered.

99. Interview with Dep't of Justice officials (Nov. 15, 2016) (notes on file with author).

sovereignty violation occurs, if at all, when a government *continues* to unilaterally search or seize extraterritorially located devices or data *after* they learn where the device or data is located, particularly in cases where what is accessed is not sufficiently targeted.

2. The EU and Council of Europe Approach

The EU and the Council of Europe also are similarly struggling to determine when, and in what circumstances, law enforcement agents can themselves seize data across borders. The Budapest Convention's Cloud Evidence Group has warned in particular about the failure to address the "loss of location" problem—warning that it is leading governments to "increasingly pursue unilateral solutions" with "unclear safeguards."[100] The Group has launched a discussion about a new protocol to the Convention in response that would, among other changes, permit "[t]ransborder access without consent in good faith or in exigent or other circumstances," with notification requirements built in.[101] A recent European Commission report has similarly emphasized the possibility of direct law enforcement access in certain circumstances.[102]

Notably, there is an already existing model for this approach within the EU. The Directive on the European Investigative Order allows an "intercepting state" to access the telecommunications of a target located within another state, so long as it provides notice to the state where the target is located.[103] This notice is to be provided in advance when possible; if the target's location is not known in advance, notice needs to be provided as soon as the location is known. The notified party then has ninety-six hours to object. If there is no

---

100. CEG REPORT, *supra* note 7, at 16–17, 45. Article 32 of the Budapest Convention explicitly authorizes a state party to directly and unilaterally access data in another jurisdiction in only two circumstances: (i) if the data is publicly available (open source); or (ii) with respect to "stored computer data located in another Party," the "person who has the lawful authority to disclose" provides his or her "lawful and voluntary consent." Convention on Cybercrime, *supra* note 70. This second provision presupposes knowledge as to where the data is stored: "Article 32b refers to 'stored computer data located in another Party.' . . . [It] would not cover situations where the data are not stored in another Party or where it is uncertain where the data are located." *See* TRANSBORDER ACCESS TO DATA AND JURISDICTION, *supra* note 67, at 19; *see also* Cybercrime Convention Comm. (T-CY), *Criminal Justice Access to Data in the Cloud: Challenges*, COUNCIL EUR. (May 26, 2015), https://rm.coe.int/1680304b59 [https://perma.cc/C8VT-VYUS] (discussion paper prepared by T-CY Cloud Evidence Group); Cybercrime Convention Comm. (T-CY), *T-CY Guidance Note # 3 Transborder Access to Data (Article 32)*, COUNCIL EUR. 6 (Nov. 5, 2013), https://rm.coe.int/16802e726a [https://perma.cc/H8T5-MQXN].

101. *Cybercrime*, *supra* note 9; CEG REPORT, supra note 7, at 45.

102. *See* Inception Impact Assessment, *supra* note 81; EUR. COMM'N REPORT, *supra* note 62, at 12–14.

103. *See* Investigation Directive, *supra* note 83, art. 31.

objection, then the interception can continue. But if the host state objects, the sought-after collection cannot go forward or must be terminated if it has already begun.[104]

This kind of compromise measure makes sense. It recognizes both the sovereign interest in accessing sought-after data in certain circumstances, regardless of the location, *and* the sovereign interest in controlling—and perhaps limiting—law enforcement activity within a state's territory in certain circumstances. And it seeks to accommodate both by placing reciprocal obligations of notice and an opportunity to object on participating states. It thus moves away from the fraught assumption that location of data necessarily controls for purposes of delimiting a state's jurisdictional reach, but also recognizes that sovereigns may have a legitimate and countervailing interest in limiting access to data that is territorially located.

II. THE RIGHT TO BE FORGOTTEN AND OTHER BROAD-REACHING PRIVACY REGULATIONS

The right to be forgotten and the related disputes about implementation raise a very different, but related, set of jurisdictional concerns. Whereas attempts by law enforcement to access data across borders primarily raise questions about the permissible scope of enforcement jurisdiction, the right to be forgotten and other related privacy-based regulations primarily raise questions about the reach of prescriptive jurisdiction. Yet, there is overlap with respect to some of the key foundational questions, such as whether and in what situations extraterritorially located providers should be subject to a state's prescriptive and enforcement jurisdiction. The right to be forgotten and other privacy regulations also—as with law enforcement requests for data—place front and center the increasingly important role of transnational corporations in mediating disputes across borders. As with law enforcement access issues, companies that hold the data are often the ones in the position of deciding which set of rules to comply with and which to resist.

I start with the right to be forgotten, and then briefly address other EU-wide privacy regulations, as reflected in the soon-to-be implemented General Data Protection Regulation.

104. *Id.*

A. The Right to Be Forgotten

In 2014, the European Court of Justice issued a landmark ruling in what is known as the *Google Spain Case*, asserting a far-reaching "right to be forgotten." The case was initiated in 2010, when Mr. Costeja Gonzalez, a Spanish national, demanded that Google remove from its search engine results links to two then-sixteen-year-old newspaper articles that announced the auctioning off of his repossessed home. These articles appeared when one typed in Mr. Gonzalez's name into Google's search engine.[105] Notably, Mr. Gonzalez never contested the truthfulness of the article. He instead asserted that the underlying debts had been resolved, that the information was therefore no longer relevant, and that he had a right to control the disclosure of such personal information, including the right to demand that it be delinked from a search of his name. Google refused to delink the articles, and the case ultimately made its way to the European Court of Justice ("ECJ").

The ECJ sided with Mr. Gonzalez. Relying on a penumbral interpretation of the Data Protection Directive then in place, it ruled that Google, as a search engine, was required to delist information that is "inadequate, irrelevant or excessive in relation to the purposes of the processing, . . . not kept up to date, or . . . kept for longer than is necessary unless . . . required to be kept for historical, statistical or scientific purposes"—even if the information is accurate.[106] It further concluded that the right applied regardless of whether or not the data subject could show any prejudice.[107] Moreover, this obligation applied even if the original provider of the information (in this case the newspaper) was permitted to make the information available on its own website. According to the ECJ, there was something unique—and potentially privacy destructive—about the "ubiquitous" information available on a search engine. In contrast to an isolated article on a single website, a search engine could reveal a "vast number of aspects of [o]ne's private life" that "without the search engine, could not have been interconnected or could have been only with great difficulty."[108]

---

105. *Google Spain Case*, *supra* note 11, ¶¶ 14–16. Mr. Gonzalez also filed an action against the newspaper, seeking that the paper remove or alter the original stories. The action against the newspaper was dismissed. *Id.*

106. *Id.* ¶¶ 4, 94. For a forceful critique of the ECJ's analysis, see Robert Post, *Data Privacy and Dignitary Privacy:* Google Spain, *the Right to Be Forgotten, and the Construction of the Public Sphere*, DUKE L.J. (forthcoming), https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2953468 [https://perma.cc/EU2Z-H44D].

107. *See Google Spain Case*, *supra* note 11, ¶¶ 4, 94.

108. *Id.* ¶ 80; *see also* Article 29 Data Prot. Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc v. Agencia Española de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, at 6 (Nov. 26,

The ECJ acknowledged that the right had to be balanced against the potentially countervailing interest of other internet users in information being made publicly available. Yet, it concluded that "as a general rule" the "data subject's rights override" those interests of other internet users.[109] If, however, the data subject is a "public figure," the countervailing interest of internet users in being able to access information is greater. For public figures, the right can be overridden if "justified by the preponderant interest of the general public in having . . . access to the information in question."[110] The court did not define who constituted a "public figure" or how one might determine whether the general public had a "preponderant interest" in the information.

On the jurisdictional questions, the ECJ also rejected Google's claim that it fell outside the Data Protection Directive because it was merely compiling information already in the public domain and therefore neither a "processor" or "controller" of data—the two categories that subjected Google to the relevant obligations. The ECJ emphasized that search engines create unique and potentially significant privacy concerns (and ones that the EU sought to regulate) and concluded that Google qualified as a "controller" of data.[111]

There are at least three notable aspects of this ruling in relation to the topic of this Article. First, the ECJ concluded the EU has broad prescriptive jurisdictional reach over search engines operating in the EU pursuant to the Data Protection Regulation, irrespective of where

---

2014), http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2014/wp225_en.pdf [https://perma.cc/UN6A-QC9U] [hereinafter Article 29 Working Party Guidelines] ("Even when (continued) publication by the original publishers is lawful, the universal diffusion and accessibility of that information by a search engine, together with other data related to the same individual, can be unlawful due to the disproportionate impact on privacy.").

109. *Google Spain Case*, supra note 11, ¶ 82.

110. *Id.* ¶ 99.

111. Specifically, the ECJ ruled that the collecting, retrieving, recording, organizing, indexing, storing, and disclosing of information that is done in order to operate a search engine constitutes the "processing" of such data, so as to bring Google within the regulation of the EU. It further concluded that as an operator of a search engine, Google is a "controller" of data, thus subjecting Google to the additional obligations imposed on data controllers. *Id.* ¶¶ 32, 41:

> The activity of a search engine consisting in finding information published or placed on the internet by third parties, indexing it automatically, storing it temporarily and, finally, making it available to internet users according to a particular order of preference must be classified as 'processing of personal data' . . . when that information contains personal data and . . . the operator of the search engine must be regarded as the 'controller' in respect of that processing, within the meaning of [the relevant Data Protection Directive].

It is now fairly well established that search engines such as Google constitute "processors" and "controllers" subject to EU data protection regulations, as well as the newly adopted General Data Privacy Regulation ("GDPR") that will go into effect in 2018. *See supra* note 63.

the search engine is headquartered or where the relevant processing and indexing of information takes place. Google argued that because the processing of the data was done by Google, Inc., which was based in the United States and not the EU, it was not subject to the EU regulations. The ECJ disagreed. In the ECJ's words, if the operator of a search engine sets up a branch or subsidiary in an EU state and that branch or subsidiary is "intended to promote and sell advertising space offered by that engine and . . . orients its activity towards the inhabitants of that Member State," it is subject to the EU's prescriptive jurisdiction.[112] Here, Google Spain, a subsidiary of Google, operated in Spain, engaged in advertising activity targeted at Spanish residents, and did so with the aim of making the Google search engine, and thus Google, Inc., profitable. It thus brought both Google Spain and Google, Inc. within the EU's jurisdiction.

Notably, the newly adopted General Data Privacy Regulation ("GDPR"), goes even a step further—expanding its jurisdictional reach to companies that serve EU residents and providers that process EU data, even if they do not have a physical presence in the EU.[113] More specifically, the regulation imposes its wide array of obligations—including the specifically mentioned right to be forgotten—on any search engine (as well as other "processors" and "controllers" of data) that is "offering . . . goods or services" to EU subjects, or "monitoring [the] behavior" of EU-based subjects.[114] Thus, whereas the ECJ grounded its prescriptive and adjudicative jurisdiction in part on the fact that Google Spain was located within a member state, the GDPR eliminates that location-based requirement. This is akin to the jurisdictional test adopted by the Belgian courts in the Yahoo! and Skype cases, and the approach of the EU in the proposed guidance note on Article 18 of the Budapest Convention, albeit limited to subscriber information. It suggests, at least within the EU, a move toward a wide-reaching approach to prescriptive jurisdiction that imposes EU obligations on companies that offer services in the EU, even if not physically present there. And it yields the possibility of territorial regulation with far-reaching extraterritorial effect.

Second, the ECJ placed the delisting obligation on Google, as the data controller in the case. (Because Google is the search engine of choice for about ninety percent of EU residents, I focus on Google's

112. *Google Spain Case*, *supra* note 11, ¶ 6.

113. GDPR, *supra* note 63, art. 3(2).

114. *Id.*; *see also* Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the 2016 General Data Protection Regulation*, 2017 BERKELEY TECH. L.J. (forthcoming), https://ssrn.com/abstract=2914684 [https://perma.cc/LB39-PKKW].

response here.[115]) This of course is not the only way to design an implementation system. The court could have, for example, insisted that the data subject had a right to an administrative review of a claimed right to be forgotten. By instead placing the obligation squarely on the search engine, the court gave Google, a private actor, an enormous amount of discretion to make the initial decisions about who constitutes a public figure, what constitutes the countervailing right to know, and how to mediate between these conflicting interests. Between May 2014 (when Google first implemented a process of reviewing such requests) and December 2016, Google received over 665,000 requests for removal, evaluated over 1.8 million URLs, and removed approximately forty-three percent of the 1.8 million URLs.[116]

In evaluating these requests, a team of lawyers and paralegals make a number of discretionary decisions about relevance of the data, the length of time it should be made available, the individual's role in society (i.e., whether they are a "public figure"), and the extent of the public's countervailing right to know. Google says that it makes these decisions "in alignment" with the guidelines developed by the Article 29 Working Party—guidelines which include a complicated set of thirteen separate factors to be considered, several of which are broken up into multiple additional questions to be evaluated.[117] And while there is the possibility of appeal to a Data Protection Agency, there is no mechanism for a member of the public to know about, let alone complain, if Google adheres to the request to delist but does so in an arguably excessive manner. In such cases, there is no record of the decisions or review mechanism by which Google's decisions can be challenged.

Moreover, in any close case, the incentives all seem tipped in favor of delisting. Under the newly enacted GDPR, failure to respect the data subject's "right" to delisting (or what the GDPR calls "erasure")

---

115. The rest of the market is split primarily between Bing (owned by Microsoft), Yahoo!, and Baidu (a Chinese-based search engine). *See Desktop Search Engine Market Share*, NETMARKETSHARE (Aug. 2017), https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 [https://perma.cc/9R65-XEGR].

116. These statistics are updated daily. *European Privacy Requests Search Removals FAQs*, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/faq/?hl=en#are_you_removing (last visited Oct. 20, 2017) [https://perma.cc/YL3Q-UUQX] [hereinafter *European Privacy FAQ*]; *see also Search Removals Under European Privacy Law*, GOOGLE, https://www.google.com/transparencyreport/removals/europeprivacy/ (last visited Oct. 20, 2017)[https://perma.cc/QQ97-KAAU]. Other search engines operating in Europe are subject to similar obligations. But as the search engine for over ninety percent of EU users, the implementation burden has fallen primarily on Google. I thus focus on Google's processes here.

117. *European Privacy FAQ*, *supra* note 116; *see* Article 29 Working Party Guidelines, *supra* note 108, at 12–20. The Working Group was set up by 95/46/EC, art. 29. Council Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995, 1995 O.J. (L 281). It is comprised of representatives from each member state, European Commission representatives, and EC institution representatives, and it operates by majority vote.

can lead to fines of up to four percent of the controller's global revenue.[118] Thus, whereas failure to delink can yield a hefty fine, excessive delinking results in no penalty. The initial decisionmaking also is made without a countervailing entity to represent either the public's right to know or the original source of the information.[119] Specific journalists can, and in fact have, learned of and protested these decisions (thus further highlighting the very data that the subject sought to make obscure), but these protests are both rare and occur after the fact, once the decision has already been made.[120]

Third, the ECJ left open the key, and still contested, issue as to the territorial scope of the announced right. How far does the obligation to delink extend? Initially, Google responded by delinking the information from the European Google Search domains (i.e., google.fr, google.de, google.es, etc.) and left it accessible elsewhere, including on google.com. The Article 29 Working Group made clear that it viewed this as insufficient:

> [L]imiting de-listing to EU domains on the grounds that users tend to access search engines via their national domains cannot be considered a sufficient mean[s] to satisfactorily guarantee the rights of data subjects according to the ruling. In practice, this means that in any case de-listing should also be effective on all relevant domains, including .com.[121]

In May 2015, the French data protection agency ("CNIL") took up the mantle of the Article 29 Working Party and ordered Google to remove delinked information from all applicable domains, including the .com domain.[122]

Google appealed, warning of the "innumerable examples around the world where content that is declared illegal under the laws of one country, would be deemed legal in others." As Google's General Counsel, Kent Walker, put it, "if French law applies globally, how long will it be until other countries—perhaps less open and democratic—start

---

118. GDPR, *supra* note 63, art. 83(5).

119. In fact, the Article 29 Working Group, which oversees implementation of the EU's Data Privacy Directive, objects to Google, or any other search engine, notifying the initial source of the information given, among other concerns, the risk that notification will result in the information being further spotlighted. *See* Article 29 Working Party Guidelines, *supra* note 108, at 3 ("Search engines should not as a general practice inform the webmasters of the pages affected . . . ."); *Id.* at 10 (warning that "[s]uch a communication is in many cases a processing of personal data and, as such, requires a proper legal ground in order to be legitimate. No legal ground can be found . . . ."); *European Privacy FAQ*, *supra* note 116.

120. *See, e.g.*, Jeffery Toobin, *The Solace of Oblivion*, NEW YORKER (Sept. 29, 2014), http://www.newyorker.com/magazine/2014/09/29/solace-oblivion [perma.cc/QW75-FNYB] (describing controversy over perceived attempts to delete links to a BBC blog post).

121. *See* Article 29 Working Party Guidelines, *supra* note 108, at 3.

122. The CNIL is comprised of seventeen members, including parliamentarians; members of the French Economic, Social and Environmental Council; representatives of high jurisdictions; and appointed "qualified public figures."

demanding that their laws regulating information likewise have global reach?"[123] Walker warns of a "global race to the bottom," ultimately resulting in French citizens being unable to see information that is perfectly lawful to view in France.[124] Google further argues that its current approach is effective in protecting the applicable right. It noted that ninety-seven percent of French users access the search engine via Google.fr—meaning that while not foolproof, the vast majority of French users would not see the link.[125]

But Google lost, and in March 2016 it agreed to a compromise measure. It now restricts access to the URL from any domain (including google.com) if the search originates in the same country as the person who requested the delinking. But it does not limit access on google.com for those searching from other locations.[126] Thus, individuals from Spain who type in Mr. Gonzalez's name will not pull up the articles about his home auction, no matter what Google domain they use to do so. Individuals in France, however, would not be able to access that information using Google.fr, although they would be able to access it if they instead used Google.com. The compromise, however, was not good enough for the CNIL. It wants Google to remove the links from all domains, regardless of the place of access. And it fined Google one hundred thousand Euros for failing to do so. After pending before France's highest administrative appeal court for months, the case has now been referred to the European Court of Justice—explicitly asking the question of whether allegedly infringing material has to be removed globally, or whether the takedowns can be limited to searches emanating from the EU.[127]

---

123. Alex Hern, *Google Takes Right to Be Forgotten Battle to France's Highest Court*, GUARDIAN (May 19, 2016, 8:20 AM), https://www.theguardian.com/technology/2016/may/19/google-right-to-be-forgotten-fight-france-highest-court [https://perma.cc/A4H3-7C5H].

124. *Id.*

125. Carol A.F. Umhoefer & Caroline Chance, *Right to Be Forgotten: The CNIL Rejects Google Inc.'s Appeal Against Cease and Desist Order*, PRIVACY MATTERS (Sept. 22, 2015), http://blogs.dlapiper.com/privacymatters/right-to-be-forgotten-the-cnil-rejects-google-inc-s-appeal-against-cease-and-desist-order/ [https://perma.cc/CQJ2-5G2Q].

126. Google uses geolocation tools to identify the location of the searcher. *See European Privacy FAQ*, *supra* note 116.

127. *See* Conseil d'État [CE] [highest administrative court], July 19, 2017, 399922 (Fr.), http://www.conseil-etat.fr/Decisions-Avis-Publications/Decisions/Selection-des-decisions-faisant-l-objet-d-une-communication-particuliere/CE-19-juillet-2017-GOOGLE-INC [https://perma.cc/3BUM-A47U]. The case has spawned an active debate and commentary. While privacy groups, free speech advocates, and academics support Google, many others disagree. *Compare* Nani Jansen Reventlow et al., *A French Court Case Against Google Could Threaten Global Speech Rights*, WASH. POST (Dec. 22, 2016), https://www.washingtonpost.com/news/global-opinions/wp/2016/12/22/a-french-court-case-against-google-could-threaten-global-speech-rights/?utm_term=.8923fa5e5261 [https://perma.cc/GVL6-LXGB] (supporting Google to avoid "a precedent that others will inevitably use to censor search results they don't like"), *with* Frank Pasquale, *Reforming the Law of Reputation*, 47 LOY. U. CHI. L.J. 515, 517 (2015) ("Such removals

This, of course, is not the first time in which France and the United States have clashed over free speech rights. The Yahoo! case over the sale of Nazi memorabilia—permitted in the United States but prohibited in France—raises many of the same issues. Although Yahoo! initially claimed that it could not technically block just French residents' access to the relevant auction site, independent technical experts revealed that it could do so with about ninety percent accuracy, and it was ordered to adopt that technological solution.[128] That, in fact, was the basic approach Google was attempting to replicate with respect to the right to be forgotten—creating a differentiated access regime. But CNIL has deemed this insufficient, asserting that individual rights will be insufficiently protected if accessible at all.

There also is some precedent for what CNIL is requesting. Pursuant to its U.S. copyright law obligations, Google, as well as other U.S.-based providers, removes infringing material from *all* domain levels, regardless of the location of the internet user. And it does so on an order of magnitude greater than the delinkings associated with the right to be forgotten. In December 2016 alone, for example, Google removed over sixty-three million URLs based on an assessment that they infringed copyrighted material. Compare this with the 1.8 million URLs delinked pursuant to the right to be forgotten in more than two-and-a-half years.[129] Put another way, in a single month there were thirty-five times more copyright-related takedowns than URLs delisted in thirty-one months based on the right to be forgotten. Moreover, whereas the information subject to the right to be forgotten is still potentially available—just so long as it is accessed some other way than

---

are a middle ground between info-anarchy and censorship. They neither disappear information from the Internet (it can be found at the original source), nor allow it to dominate the impression of the aggrieved individual."); *see also* Farhad Manjoo, *"Right to Be Forgotten" Online Could Spread*, N.Y. TIMES (Aug. 5, 2015), http://www.nytimes.com/2015/08/06/technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=1 [https://perma.cc/XAC5-PSMF] (citing proponents on both sides).

128. *See* La Ligue Contre le Racisme et L'Antisésmistisme (L.I.C.R.A.) et L'Union des Étudiants Juifs de France (U.EJ.F.) c. Yahoo! Inc. et Société Yahoo! France Interim Court Order, Tribunal de grande instance [TGI] [ordinary court of original jurisdiction] Paris, Nov. 20, 2000 (Fr.). Ultimately, however, Yahoo! caved, adopting a new policy that applied across the board (and thus did not require filtering by geography) and would "no longer allow items that are associated with groups which promote or glorify hatred and violence . . . [including] Nazi militaria and KKK memorabilia." Jeff Peline, *Yahoo to Charge Auction Fees, Ban Hate Materials*, CNET (Mar. 29, 2002), https://www.cnet.com/uk/news/yahoo-to-charge-auction-fees-ban-hate-materials/ [https://perma.cc/3JQK-T4J7].

129. *Requests to Remove Content Due to Copyright*, GOOGLE, https://transparencyreport.google.com/copyright/overview (last visited Oct. 20, 2017) [https://perma.cc/JQ5Q-5AGZ].

via a search of the subject's name—information subject to copyright-based takedowns are removed from *all* parts of Google's site.[130]

There are, however, two key differences between the copyright rules and the right to be forgotten as they are currently being applied. First, the companies applying the copyright laws are mostly U.S.-based and thus clearly bound by applicable U.S. law. One would similarly expect Baidu, the Chinese-based search engine, to be bound by takedown orders imposed by Chinese law. The analogous conflicts emerge if every other country where Baidu operates *also* tried to impose its vision of what information should and should not be accessible from the site.[131]

Second, and importantly, there is much greater international consensus on what constitutes copyright infringement than on the right to be forgotten, where there is a significant divergence of approaches. The Berne Convention, which sets international standards for intellectual property protection including copyright, has over 171 signatories.[132] While there remain sources of dispute, there is also a fair amount of agreement. By comparison, it is hard to imagine even just the EU and the United States reaching consensus as to what constitutes a legitimate basis for content takedown given the divergent approaches

130. An analogous dispute is playing out in Canada and the United States, with Google contesting a court order requiring it to delink all websites used by a company found to have engaged in trade secrets and trademark violations. Google, as in the dispute with the CNIL, delinked the websites from google.ca, but left them up on all other domain names. But the Canadian Supreme Court deemed this insufficient and ordered Google to abide by its order across all of its domains. Google Inc. v. Equustek Solutions Inc., 2017 SCC 34, para. 41 (Can.), https://scc-csc.lexum.com/scc-csc/scc-csc/en/16701/1/document.do [https://perma.cc/L6VT-REMU]. On November 2, 2017, a U.S. district court granted a preliminary injunction prohibiting enforcement and adopting Google's position that the Canadian Supreme Court ruling "threatens free speech on the global Internet." Google LLC v. Equustek Sols. Inc., No. 5:17-cv-04207-EJD, 2017 WL 5000834, at *5 (N.D. Cal. Nov. 2, 2017); *see also Canadian Court Order Censoring Everyone's Google Search Results Must Be Overturned, EFF Tells Supreme Court of Canada*, ELECTRONIC FRONTIER FOUND. (Oct. 5, 2016), https://www.eff.org/press/releases/canadian-court-order-censoring-everyones-google-search-results-must-be-overturned-eff [https://perma.cc/58MB-N9QQ].

131. There is an interesting and related question as to whether individuals have a First Amendment right to have their speech available on particular search engines. A recent New York District Court case says no. *See* Zhang v. Baidu.com, Inc., 10 F. Supp. 3d 433 (S.D.N.Y. 2014) (rejecting First Amendment challenge against Baidu brought by U.S.-based promoters of democracy in China who claimed Baidu prevented their content from appearing on its search engine).

132. *See* Berne Convention for the Protection of Literary and Artistic Works of September 9, 1886, July 14, 1967, 828 U.N.T.S. 221. There is, however, not total consensus as to what constitutes infringing material with respect to copyright or the scope of other intellectual property protections. In fact, such disagreements have been the subject of high-stakes disputes and litigation. *See, e.g.*, *Equustek Solutions Inc.*, 2017 SCC 34; Hamza Shaban, *How a Supreme Court Case in Canada Could Force Google to Censor Speech Worldwide*, WASH. POST (June 29, 2017), https://www.washingtonpost.com/news/the-switch/wp/2017/06/29/how-a-supreme-court-case-in-canada-could-force-google-to-censor-speech-worldwide/?utm_term=.2945a2829ca7/ [https://perma.cc/7NP4-QABC].

to free speech—let alone the range of other nations that might want to assert additional bases for content takedown based on potentially offensive, unpopular, or political speech.

Meanwhile, the lack of clear standards with respect to what constitutes legitimate grounds for asserting the right to be forgotten means that companies such as Google are increasingly the ones setting the rules—and thus determining the scope of available information on a near-global scale. And because the decisions are discretionary and made by a private company behind closed doors, it is hard to know how these decisions are being made. While the data subject will know if his or her request is denied, the broader public will likely not know if it is granted, and thus has no mechanism for asserting a countervailing right to be informed.[133]

B. Privacy Regulations—the GDPR

The European Union's recently adopted and far-reaching new data protection regulation—the General Data Protection Regulation ("GDPR")—will take effect in May 2018. In addition to the right to be forgotten, the GDPR mandates a number of additional privacy and data protection measures. Among other things, it increases the number of disclosures that must be made before an entity can process personal data;[134] lays out specific limitations on the cross-border transfer of data; imposes relatively strict "consent" requirements for the processing of certain personal data;[135] restricts the scope of permissible "profiling";[136] obliges a range of companies to appoint data protection officers;[137] and includes new breach notification requirements.

As already described, these obligations have broad territorial reach, covering entities that process the personal data of EU subjects, irrespective of the location of the processor or controller, so long as the processing activities are related to the "offering of goods or services" to

133. *See* Steven M. LoCascio, Note, *Forcing Europe to Wear the Rose-Colored Google Glass: The "Right to Be Forgotten" and the Struggle to Manage Compliance Post* Google Spain, 54 COLUM. J. TRANSNAT'L L. 296, 304–11 (2015) (raising concerns about the amount of power being delegated to private companies to determine the scope of the right to be forgotten).

134. *See, e.g.*, GDPR, *supra* note 63, art. 15.

135. *See id.* arts. 7, 9.

136. *See id.* arts. 22, 24, 60, 63, 71, 73.

137. The obligation applies to those companies that engage in the "regular and systematic monitoring of data subjects on a large scale" or large-scale processing of "special categories of data." *Id.* art. 37; *see also id.* art. 39 (laying out responsibilities of data privacy officers). Although initial drafts limited the obligation to companies of 250 employees or more, later regulations lifted that limit. *See* Rita Heimes, *Top 10 Operational Impacts of the GDPR: Part 2*, INT'L ASS'N PRIVACY PROFS. (Jan. 7, 2016), https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/ [https://perma.cc/C76G-FSXG].

EU subjects, or "the monitoring of [the] behavior" of EU-based subjects.[138] The GDPR thus represents one of an array of privacy regulations with extraterritorial reach, applying its prescriptive obligations not just on locally based companies but on companies around the world that process EU subject data. Some of these requirements can, as a matter of technology and practice, be implemented in a way that is territorially limited (as Google is attempting to do with respect to the right to be forgotten). But others, such as the requirement of a data protection officer and the implementation of protections required in order to transfer data across borders, mandate the adoption of new procedures and protections that cannot easily be constrained by territory. Any company that wants to do business in the EU or transfer personal data out of the EU needs to comply with these requirements or be subject to potentially large fines.[139]

This is in many ways the EU equivalent of the U.S. requirement that all foreign governments get a U.S. warrant to obtain communications content for law enforcement purposes, regardless of the particular equities at stake.[140] With respect to the warrant requirement, the United States is imposing its substantive and procedural warrant rules on the rest of the world—or at least any part of the rest of the world that wants access to U.S.-held communications content. With respect to the privacy regulations, the EU is using its power as a key market to similarly impose its vision of appropriate privacy regulations globally—not just with respect to the right to be forgotten but with respect to a range of other privacy regulations as well. It is an example of what Professor Anu Bradford has coined the "Brussels effect"—the international version of the so-called "California effect"—defined as local regulations with broad extraterritorial effect.[141] While not exactly the kind of global governance the unterritorialists once advocated, it yields some of the same effects, but via local, territorial controls, and mediated by the global corporations that manage our data.

---

138. GDPR, *supra* note 63, art. 3(2).

139. This is part of a broader trend. *See, e.g.*, Dan Jerker B. Svantesson, *The (Uncertain) Future of Online Data Privacy*, 9 MASARYK U. J.L. & TECH. 129, 131 (2015) ("[W]hile exceptions can be found (e.g. current Japanese data privacy law), there is a tendency of data privacy laws around the world to adopt an extraterritorial scope so that European businesses doing business in Australia or Singapore will be bound to abide by Australian and Singaporean data privacy law." (citation omitted)).

140. *See* discussion *supra* Section I.A.

141. *See* Bradford, *supra* note 12, at 3.

III. IMPLICATIONS

Having detailed specific areas in which these key jurisdictional disputes are playing out, I now step back and examine some of the broader themes and challenges that emerge. In so doing, I make three key points.

First, territorial sovereigns continue to govern the internet, but what is territorial and what is extraterritorial remain in sharp dispute. Contrary to the claims of some, the distinct attributes of data and the way it is managed raise unique considerations.[142] Simply applying the rules governing other tangible and intangible assets is both unsatisfying and unworkable. Not only are many of those rules themselves unsettled and contested in key respects (particularly with respect to intangible assets), but also there are key differences between the management of personal data and things like patents, trademarks, copyrights, and dollars. We need an understanding of how the relevant attributes of data map onto the underlying normative goals that the jurisdictional rules are trying to satisfy. Otherwise, we risk blithely applying existing rules to a new medium in ways that fail to serve, or potentially even undermine, the underlying goals.

Second, territorial-based regulations are increasingly having an extraterritorial effect, providing a new form of global governance (or at least attempted global governance), but via unilateral rulemaking. Such forms of unilateral, extraterritorial rulemaking provide an opportunity for states to use their leverage to prod international partners to adopt the normative vision of the regulating state. This can be used to encourage partner nations to be more rights or privacy respecting, even in the absence of the kind of consensus that might lead to direct bilateral or multilateral agreements. But it can also be used to impose one set of values and preferences on others—in ways that cause clashes and increasingly potent conflicts of laws. This of course is neither a new phenomenon nor one that is unique to the field of data regulation, but it is an issue that has particular resonance here given the potentially profound implications for privacy, speech rights, security, and democratic governance.

Third, key decisions as to whose rules apply and how they are interpreted are increasingly being determined not by states, but by the major multinational companies that operate across borders. In making basic decisions about where to locate data and personnel, how to design systems, and when to fight versus when to comply with court orders, private companies are increasingly setting and interpreting the rules.

142. *See, e.g.*, Woods, *supra* note 13, at 754–64.

At times they are being explicitly delegated the authority to do so.[143] All of this has significant implications for privacy, security, and speech rights, as well as the relationship between the government and the governed.

A. Defining Territoriality

The grand vision of a new global order to regulate the global—and unterritorial—medium of data flowing across the internet has not come to pass. Rather, states have and will continue to find ways to assert territorial-based controls on the data and providers that pass through or operate in their states. (And this reality has its benefits, particularly with respect to privacy rights.[144]) But what is territorial and what is extraterritorial remains in sharp dispute, reflecting the challenges and opportunities that arise from the efforts to impose territorial-based controls on what is inherently an unterritorial medium. In what follows, I highlight the relevant features of data that need to be taken into account and then suggest how these features do and should shape our assessment of what is territorial in the realm of both enforcement and prescriptive jurisdiction.

1. Data's Differences

In an earlier article, I highlighted features of data that challenge our conceptions of what is territorial and what is unterritorial.[145] In a recent *Stanford Law Review* article, Professor Andrew Keane Woods takes aim at my categorization of data as different.[146] In his view, nothing is particularly new; we should simply look to the ways jurisdictional issues have been worked out with respect to analogous forms of both tangible and intangible property and we will have all the answers needed.[147] Woods, however, mischaracterizes my key point and glosses over the salient features of data that are creating the kinds of conundrums this Article and prior work seeks to address.

---

143. *See supra* Section II.A.

144. *See, e.g.*, Stephen J. Schulhofer, *An International Right to Privacy? Be Careful What You Wish For*, 14 INT'L J. CONST. L. 238, 254–59 (2016) (warning that any attempt to reach mutually agreed upon, globally applicable common ground on both privacy and speech rights will almost certainly yield a race to the bottom versus the top and thus an ultimate reduction in core privacy and speech rights for many); *see also* Daskal, *supra* note 13, at 395 (same). That said, there may be the possibility of bilateral or multilateral cooperation, at least on some discrete issues. *See* discussion *supra* Section I.A.4.b.

145. Daskal, *supra* note 13, at 365–77.

146. Woods, *supra* note 13, at 729, 734, 755.

147. *Id.* at 756–63, 764–74.

First, contrary to Woods' argument, the claim that data is different and that these differences challenge our assessment of territoriality is *not* the same as saying that territorial-based efforts to control and regulate are or should be jettisoned. Rather, it is an acknowledgment that data raises difficult questions about the basic understanding of what is a territorial versus extraterritorial basis of jurisdiction with respect to data. Second, in focusing on the similarities between data and other forms of tangible and intangible property—of which there are of course many—Woods glosses over the key differences. It is for good reason that numerous governments, academics, and judicial bodies are actively struggling to define the key jurisdictional limits to both enforcement and prescriptive jurisdiction over data. The answers are not at all clear.

In what follows, I briefly reiterate the attributes of data I highlighted in previous work—namely its mobility, divisibility, location independence, and fact of third-party control—explain why these attributes matter and counter the argument that it is nothing new.

First, data's mobility: as Woods points out, data is not the only kind of property that is highly mobile.[148] People and other forms of tangible property cross borders. But both humans and other forms of tangible, tactile property do so in relatively predictable, observable ways. Data by contrast moves at the speed of light, in ways that are totally unpredictable and generally unknown to both the data subject and the governments seeking to access sought-after data. This, both independently and in conjunction with the other unique features of data described below, makes data location a particularly unstable basis for defining territoriality or delimiting enforcement jurisdiction.

It also means, as we have seen in the discussions of the *Microsoft Ireland* case and blocking provisions imposed by U.S. and EU law, that jurisdictional rules that turn on the location of data fail to serve key normative and practical interests at stake.[149] Simply put, there is an increasing mismatch between where data happens to be located and the sovereign and other relevant interests at stake. As a practical matter, such a rule fails to address what the EU describes as "loss of location"—meaning that in many cases neither the state nor the data subject knows the relevant location of data at any given point in time.[150]

148. *Id.* at 758.

149. *See* discussion *supra* Section I.A.

150. As discussed earlier, Google, for example, moves data around by algorithm, based on an array of performance, reliability, and other efficiency concerns. *See In re* Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708, 712–13 (E.D. Pa. 2017); *In re* Search of Content that is Stored at Premises Controlled by Google, No. 16-mc-80263-LB, 2017 WL 1487625, at *2 (N.D. Cal. Apr. 25, 2017).

Second, data's divisibility: it is true, as Woods points out, that even if people and other goods cross borders in a more predictable, plodding manner, there are other assets, like money and debt, that operate as a form of data and thus move around the globe at the speed of light.[151] According to Woods, we should therefore simply look to the jurisdictional rules governing money.[152] But there is also a key difference between rapidly moving communications content and rapidly moving money. Money and debt are rivalrous assets. They can only be held (even if converted into 0s and 1s on a bank's balance sheet) in a single location at a time. Data, by comparison, can be unilaterally copied and held in multiple jurisdictions at once, without altering in any meaningful way the nature of the data or the data subject's ability to access or manipulate it. This distinction matters.

Let's consider one of Woods' key hypotheticals. Woods points to the fact that the ten dollars that John Smith deposits in the bank is not likely the same ten dollars he receives when he later withdraws the money. The particular ten dollars has likely been divided and distributed and might have even been exchanged for foreign currency.[153] But, critically, there is still a single ten dollars—in whatever form—linked to John Smith. John Smith's money may have been divided and re-distributed, but it cannot be multiplied, at least not without the bank or John engaging in some sort of fraudulent activity. If John Smith's ten dollars is seized by a government, it is no longer available to him. Or if John Smith later withdraws his ten dollars in the equivalent amount of pesos in Mexico, he cannot later also withdraw the ten dollars in the United States.

Data is different. It can be divided, distributed, multiplied, accessed, copied, and subsequently manipulated by multiple different parties, without in any way interfering with the original data subject's ability to use or access it. It can, for example, be held in multiple different jurisdictions and be subject to simultaneous seizure by multiple different law enforcement agencies in a way that money, debt, or other forms of property cannot. It can be "seized" by State A, yet still available, unaltered in any meaningful way, for State B to simultaneously or subsequently seize.

This matters to both the enforcement and regulatory jurisdictional issues addressed in this Article. Whereas law enforcement agents in State A might have a legitimate sovereign interest in protecting $10,000 from a locally held bank account being

151. *See* Woods, *supra* note 13, at 758–59.

152. *Id.* at 759–60.

153. *Id.*

siphoned off by State B, the sovereign interest that is impinged upon by the mere act of copying a piece of data is minimal, to the extent it exists at all. A state's sovereign interests arise from *other* equities than the need to ensure access for itself—perhaps, for example, an interest in protecting the privacy of one's own citizens and residents or a normative interest in baseline privacy protections. Understanding these underlying equities is critical to the development of sound jurisdictional rules.

The divisibility of data also matters for another reason. It means that a particular source of data, or link on a search engine, can be taken down from one domain (such as google.es) without in any way changing the ability to access the same information from another server where it might be held on another domain (such as google.com). Conversely, it means that if it is not *also* taken down from google.com, or deleted more widely, it can likely be accessed by some, including at least some subset of the population that a government might want to prevent from accessing it. This obviously has important implications for the regulation of copyright infringement, libel, terrorist use of the internet, and, of course, the right to be forgotten. States seeking to limit access to content in these situations have one of two choices. They can accept that territorial-based limits on speech come with the possibility of evasion. Or they can, as the CNIL is doing, insist that the infringing content be deleted from all applicable servers or delinked from all search engine domains—and in so doing impose its normative vision on a global, or near-global, scale.[154]

Third, location independence: data can be accessed and manipulated remotely. This means that a data subject can be separated from the data he or she is manipulating by an international border. It also means that both law enforcement agents and service providers acting as agents of law enforcement can access data across borders without ever setting foot in the foreign country. Once again, there are similarities with money. One might live in the United States and store one's money in an offshore account but access it from an ATM in New York City. But there is a key difference that ties back to data's divisibility: once money is accessed and retrieved, it is no longer available in that offshore account. Law enforcement can, by contrast, access and copy data without excluding others or interfering with the data subject's ability to access it.

154. *See, e.g.*, Paul Schiff Berman, *Global Legal Pluralism*, 80 S. CAL. L. REV. 1155, 1159–60 (2007) (making a similar point with respect to France's case against Yahoo! over the availability of Nazi memorabilia and Holocaust denial material).

Location independence also matters to our understanding of both prescriptive and enforcement jurisdiction. Providers based exclusively in State A can provide a whole host of services in State B without ever setting foot in State B. Evolving jurisdictional rules seek to reflect this reality; states are concerned that providers will escape regulation and other legal responsibilities simply because they are not territorially located there. In response, Belgium's assertion of jurisdiction in the Skype and Yahoo! cases, EU's new GDPR regulations, and the Council of Europe's proposed guidance on Article 18 of the Budapest Convention all adopt broad-reaching assertions of both prescriptive and enforcement jurisdiction that focus on the place where providers "orient" their activities or offer their services, rather than the place where either the provider or data is located. This also tracks the way U.S. courts have been establishing jurisdiction over internet providers in a range of civil cases.[155] It also increases the likelihood of territorial-based regulation with broad extraterritorial effect.

Fourth, third-party control: the location of data is increasingly controlled by third parties, as exemplified by the *Microsoft Ireland* case. The user generally does not pick the location where it is held, and thus there may be no normative link between a data subject and the location where his or her data happens to be held. This is a very different situation than when one purchases a house in, physically travels to, or opens an offshore bank account in a particular location. In those situations, one chooses the place and implicitly agrees to abide by the relevant jurisdiction's law, even if it is a remote jurisdiction. With data, there is often no equivalent choice being made by the relevant property owner and thus no notice about, or control over, the rules that potentially govern access to the data.

This has two key implications. First, it raises concerns about fair notice and accountability. If users do not know where their data is located and thus who has control over it, they have no way of holding governments accountable. Second, it means that in the absence of mandatory data localization requirements, transnational corporations—rather than either data holders or governmental actors—make the key decisions about where to locate data, and thus, to the

155. *See, e.g.*, Zippo Mfg. Co. v. Zippo Dot Com, Inc., 952 F. Supp. 1119, 1124 (W.D. Pa. 1997) (establishing what is known as the "Zippo test"—a sliding scale test for establishing jurisdiction on the Internet based on the degree of contract between the plaintiff and company's website). Several circuit courts have since adopted either this or a modified version of this test. *See, e.g.*, Gator.com Corp. v. L.L. Bean, Inc., 341 F.3d 1072, 1079 (9th Cir. 2003); ALS Scan, Inc. v. Dig. Serv. Consultants, Inc., 293 F.3d 707, 714 (4th Cir. 2002); *see also* Mark A. Lemley, *Place and Cyberspace*, 91 CALIF. L. REV. 521, 529–30 (2003).

extent that data location governs, the rules that apply. EU efforts—under both the current Data Privacy Regulation and soon-to-be implemented GDPR—to demand the implementation of basic privacy protections as a condition for permitting the flow of data outside the EU's borders represent a direct response to this reality, reflecting an effort to reassert territorial control by limiting the flow of data from the EU to elsewhere absent some "adequacy" determination with respect to the privacy rules and security protections in place.

These attributes of data, both individually and collectively, matter to the assessment of the relevant sovereignty and other key interests at stake; this in turn should be taken into account in determining the jurisdictional rules that apply. I turn to this task now.

2. Territoriality and Enforcement Jurisdiction

What is clear from this discussion is that the simple mapping of rules governing other forms of tangible and intangible property does not work either practically or normatively. Whereas there is a clear international law prohibition on law enforcement in State A unilaterally accessing property in State B, an equivalent rule with respect to data creates a mismatch between the underlying sovereign interests and jurisdictional rules that apply. In response, states have developed a smorgasbord approach to assessing enforcement jurisdiction—with some continuing to reify the location of data, others focusing on the location of the provider that controls the data, still others looking to the place where data is either received or disclosed, and some adopting a combination of the above. What is needed is a better mapping of the jurisdictional rules with the sovereign and other normative interests at stake. This in turn requires a theory of what does and does not constitute a legitimate sovereign interest and what other relevant interests should be considered—a tricky, contested, and complex set of issues.

For these purposes, I offer an initial assessment of the key interests at stake—recognizing that such an assessment is itself deserving of its own series of articles and books. My goal here is to simply outline *how* one would think about these interests in connection to the relevant jurisdictional rules; the *specifics* will shift depending on one's assessment of these baseline claims and their relative importance.

With those caveats in mind, I proffer that there are, as a general matter, at least five key interests at stake with respect to law enforcement efforts to access data. First, states have a sovereign interest in preventing and prosecuting crime. Second, states have a sovereign interest in protecting their citizens and residents, and thus

limiting or controlling the ability of foreign governments to unilaterally access citizen or resident data. Third, states have a broader interest in setting baseline substantive and procedural protections to govern access to data globally—an interest justified both by normative preferences and by the narrower interest of protecting citizen and resident data that might be intermingled with a legitimate foreign target's data. Fourth, states have an interest in protecting the economic interests of local companies. And fifth, separate and apart from the state interest, the individual data subject has an interest in protecting his or her privacy, protecting against abuse, and having some knowledge and control (via democratic processes or otherwise) over the rules that apply.

A location-of-data test, such as that provided by the *Microsoft Ireland* case or U.S. blocking provisions, fails to serve most of these key interests. First, it stymies law enforcement access to data in legitimate investigations based simply on where the data happens to be held. In most cases, those location decisions are based on providers' efforts to maximize efficiency and reduce cost, rather than other normative considerations. Second, a location-based rule fails to reflect the state's interest in protecting its own residents and citizens and instead sets arbitrary limits on a government's ability to access data based on business decisions of providers. Third, such a rule does nothing to promote the development of baseline rules; rather, it simply defers to the procedural and substantive rules that apply in the nation where the data is located, no matter how weak they are. Fourth, to the extent that a location-based rule encourages data localization mandates as a means of ensuring local law enforcement access, such rules are harmful both to the future growth of the internet and to the state's own providers. In requiring providers to cache local copies of data, governments significantly increase the costs of doing business for providers that operate multinationally and potentially price startups out of the international market.

The one key interest that is potentially aided by such a location-based rule is notice to the data subject, which can help the individual user protect his or her privacy (the fifth interest outlined above). One could imagine that, if a location-based jurisdiction approach became the stable norm, data subjects would increasingly demand notice and choice regarding data location. This would require a shift in practice; as of now, most users that rely on third-party providers to store or manage their data lack notice, choice, and even the ability to ascertain where

their data is located at any given moment.[156] If implemented widely, however, a location-based approach would provide some increased predictability as to the rules that apply, which in turn would provide the clarity needed to protect privacy and prevent abuse, albeit at the cost of other key interests.

Conversely, a give-us-everything approach, as exemplified by the Belgian courts' approach to enforcement jurisdiction, advances the sovereign interest in investigating and prosecuting crime but fails to serve other relevant, key interests. In setting a standard that any state can demand the production of data of anyone, anywhere, this approach fails to respect other states' countervailing interests in limiting or controlling foreign government access to their own citizens' or residents' data. It fails to provide any kind of baseline procedural or substantive protection; rather, all that matters is that the state claims a justification for accessing the data. It also imposes economic risk on locally based providers that operate multinationally; given the continued reality of blocking statutes, such an approach puts providers at risk of being caught in the middle of two conflicting legal obligations, with one state asserting the right to access data and the other prohibiting such disclosure. Finally, it fails to serve the individual interest in either notice or choice; users will likely have no way of knowing or controlling when governments access their data and for what reasons, absent a voluntary decision on the part of the provider to disclose.[157]

Discussions in the EU and Council of Europe, as well as draft legislation in the United States, recognize the need for a more nuanced approach that mediates between these two extremes. While still in their beginning stages, these efforts seek to better balance the competing interests at stake and reflect a growing awareness of the value of harmonizing approaches across borders.[158] In particular, the approach taken by the United States in negotiations with the United Kingdom,

---

156. A company like Microsoft is starting to provide such location-driven options, particularly with respect to its enterprise customers that want, or are required by local law, to keep data locally. But this is not possible for a company like Google or Facebook—at least not without a major overhaul of their business. These companies regularly move data for a whole host of productivity and efficiency reasons and thus cannot easily ensure that customers' data remain in any one particular location or give customers such locational choices. *See In re Search Warrant*, 232 F. Supp. 3d at 724–25.

157. Of additional concern, providers are often explicitly barred from informing their customers that their data have been seized. While a temporary prohibition on disclosure often makes sense as a means of protecting the integrity of an investigation, indefinite bars on disclosure are not. For a discussion of these issues, at least under U.S. law, see Jennifer Daskal, *Notice and Standing in the Fourth Amendment: Searches of Personal Data*, 25 WM. & MARY BILL RTS. J. (forthcoming 2018).

158. *See* discussion *supra* Section I.A.4.

and the accompanying draft legislation, reflects the key interests identified. Such an approach seeks to ease limits on law enforcement access to communications content, thus better facilitating the ability to investigate and prosecute crime. Yet it also recognizes that states have a legitimate interest in restricting access to their own citizens' and residents' data. Moreover, it demands the application of baseline substantive and procedural rules as a precondition to access, thereby reflecting the normative interest in minimum privacy interests and the more self-serving interest in protecting the data of the state's own citizens that might be intermingled (incidentally collected) with the data that a foreign government is requesting. This approach is of course not perfect, as virtually nothing in this area will be. There are, for example, active and ongoing debates about the particular procedural and substantive standards required.[159] And it is unclear whether and how such an approach could be scalable beyond a relatively small handful of like-minded nations.

But it is nonetheless a step forward. If enacted, the legislation would represent a much better alignment of the jurisdictional rules with the relevant interests at stake than currently exists. It reflects an effort to facilitate states' legitimate interest in investigating and prosecuting crime, while also respecting states' interests in controlling access to their own citizens' and residents' data. It seeks to harmonize approaches across borders, thus minimizing conflict and reducing the likelihood that companies will be caught in a conflict of laws. And it uses the United States' leverage as the holder of so much of the world's data to push norm development in ways that ultimately inure to its citizens' and residents' benefit, even if they are not the direct target of a foreign government's search or seizure.[160] If successful, it could provide a model for reform efforts elsewhere.

* * *

Remote searches of extraterritorially located data and devices performed directly by law enforcement also raise a similar set of challenges to our assessment of what is territorial, what is extraterritorial, and what constitute the key sovereign interests at stake. The prospect of law enforcement officials reaching across borders, albeit remotely, to unilaterally access property in another jurisdiction is both disconcerting and widely deemed a violation of sovereignty. At the same time, it is hard to explain why the *inadvertent*

159. *See supra* note 44 and accompanying text.

160. *See* discussion *supra* Section I.A.4.c.

accessing and copying of data that happens to be located in a foreign jurisdiction is inherently a sovereignty violation, particularly if coupled by after-the-fact notice once the data location has been discovered.

The approach suggested by the Cloud Evidence Group seems to recognize this. It would explicitly authorize cross-border searches by law enforcement if inadvertent or in an emergency situation.[161] Notice to the host government if and when it becomes apparent that the data or device is outside the acting state's territorial jurisdiction would be required.

A similar set of rules also should be enacted by the United States to deal with the possibility of remote searches reaching extraterritorially located data or devices pursuant to the recent revisions to Rule 41 of the Federal Rules of Criminal Procedure. Notice to the target government generally should be required. If the target government objects, the searching government should be obliged to abandon or cease its activity in such a situation and possibly be prohibited from introducing already seized data in a criminal case.

That said, there may be times when it would unduly jeopardize an investigation to notify the host government of the law enforcement actions taken. Here, I would borrow from the international law on countermeasures, as articulated in the 2001 Articles on State Responsibility.[162] The default rule is that if State A is planning certain actions known as countermeasures in State B, State A is required to notify State B in advance.[163] If, however, "urgent countermeasures . . . are necessary to preserve [the state's] rights," notice is not required.[164] The commentary notes that notice can be suspended if it would "frustrate" the acting state's purposes.[165]

For obvious reasons, there are situations in which notification of hacking activities to the target country would similarly frustrate the legitimate law enforcement activities of the notifying state. Consider, for example, a situation involving state-sponsored or state-sanctioned illegal activity. Notice to the target state would risk upending the investigation. In those narrow situations, states should be permitted to engage in no-notice searches without running afoul of international law. That said, notice and cooperation should be the rule.

In sum, the jurisdictional rules governing law enforcement access to data—both with respect to compelled disclosure orders and

161. *See* discussion *supra* Section I.B.2.

162. Int'l Law Comm'n, Rep. on the Work of Its Fifty-Third Session, U.N. Doc. A/56/10 (2001).

163. *Id.* art. 52(1).

164. *Id.* art. 52(2).

165. *Id.* art. 52, cmt. 6.

efforts at direct access—should map as closely as possible onto the sovereign and related interests at stake. These interests are themselves in internal tension, exacerbating the difficulty of this task. But a few things seem clear: A test that focuses exclusively on the location of data fails to reflect the actual attributes of data in ways that are incongruent with the relevant interests at stake. Conversely, a test that gives law enforcement access to whatever it deems relevant to an investigation, without regard to countervailing considerations, is not a satisfactory answer either. Such an approach fails to take into account the countervailing sovereign interests in limiting access to citizens' and residents' data and controlling foreign state activity in their borders. It also fails to reflect both the sovereign and broader normative interests in setting baseline procedural and substantive protections as to the rules that apply. The goal should be a set of jurisdictional rules that fall in between these two approaches—ones that reflect both the legitimate sovereign interest in sometimes accessing data outside a state's borders and the countervailing interests in limiting access to citizens' and residents' data; promote the implementation of baseline substantive and procedural privacy protections; and facilitate user notice with respect to the rules that apply.

3. Territoriality and Prescriptive Jurisdiction

The questions of prescriptive jurisdiction are much less contested than those involving enforcement jurisdiction. A range of developments in the EU, Council of Europe, ECJ, and elsewhere suggest an increasing consensus in favor of broad reach of prescriptive jurisdiction to cover a provider offering services in one's territory, even if the provider does not have a territorial presence in terms of personnel or place of operations. This reflects the fact that providers increasingly can manage data across borders and have local effect without ever setting foot in the territory where their data is located—a consequence of what I call location independence.

While providers have at times contested the wide scope of prescriptive jurisdiction, they have generally consented to the states' jurisdiction to adjudicate such claims. In the Yahoo!, Skype, and right to be forgotten cases involving Google, for example, major multinational corporations have appeared in court and paid fines and other penalties when ordered to do so.[166] And this is perhaps wise. After all, states have all kinds of tools to enforce compliance, even in situations where the provider is not physically located in their territory. States can, for

166. *See supra* Sections I.A.1, I.A.2, II.A.

example, block the availability of certain services; prohibit residents from using certain services; or seek, via mutual cooperation, seizure of assets with the assistance of states where the provider is physically located.[167] The result of such broad assertions of jurisdiction is the growing phenomenon of extraterritorial regulation via territorial rule. It is to these developments that I now turn.

B. Extraterritorial Regulation via Territorial Rulemaking

The interconnected nature of data, the transnational workings of the providers that control and manage our data, and broad assertions of prescriptive jurisdiction together yield opportunities for states to regulate with far-reaching extraterritorial effect. This has several implications of importance for the issues discussed here. First, whereas the unterritorialists' vision of new supranational institutions to regulate the internet has not come to pass, there is an alternative form of international standard-setting via local regulation now taking place.[168] It is what Professor Anu Bradford has coined the "Brussels effect"—the international version of the so-called "California effect," pursuant to which California's regulatory practices set standards ultimately applicable across other states, even if not mandated by other states or the federal government.[169] It operates this way: regulation in one state yields the adoption of uniform standards that have far-reaching effects, far beyond the boundaries of the regulating state.

The EU's broad assertions of privacy and security regulations that reach every company that processes EU residents' data is an obvious example. The GDPR's required appointment of a Data Protection Officer, for example, is likely to yield privacy benefits that extend far beyond the territorial boundaries of the EU.[170] Data security requirements will have wide-spread effects as well.[171] Rules demanding "adequate safeguards" before personal data can be transferred outside the EU also indirectly impose EU-style privacy standards on just about any company that wants to operate globally, including within the EU.[172]

---

167. *See* GOLDSMITH & WU, *supra* note 2.

168. *See* Bradford, *supra* note 12, at 5. As Bradford points out, such efforts work best when there is, among other things, a strong domestic market (here the EU), significant regulatory capacity, and nondivisible conduct or production, meaning it is not feasible or viable for private sector actors to maintain different standards across different markets. *Id.*

169. *See* Danielle Keats Citron, *The Privacy Policymaking of State Attorneys General*, 92 NOTRE DAME L. REV. 747 (2016) (describing in detail how California's privacy policies were exported across the United States).

170. *See, e.g.*, GDPR, *supra* note 63, arts. 37–39.

171. *Id.* arts. 32–34.

172. *Id.* art. 45.; *see also id.* arts. 44, 46.

Copyright rules imposed by the United States and implemented by U.S. companies offer another example, with the United States' vision of what constitutes infringing material—and thus what is subject to takedown requests—being imposed on the rest of the globe via the operations of U.S.-based providers.

This provides a new form of international rulemaking, but through the de facto operation of the market and the multinational corporations that operate across borders—rather than the more formal and mutually agreed upon process of treaty making amongst states or international organizations setting standards that impose obligations on participating states. In many instances, multinational companies that operate across borders, sub silentio, adapt to the more stringent regulations in ways that ultimately apply to all of their operations, and not just the operations in the regulating state.

Other times, regulations in one state can effectively coerce another state to adapt. EU-wide restrictions on transferring personal data outside the EU, for example, have led the United States to adopt new rules and regulations designed to protect the free flow of data from the EU to the United States. The extension of the Judicial Redress Act to cover Europeans was a direct response to the demands of the Europeans in this regard. The interest in preserving the free flow of data also incentivized the adoption of Presidential Policy Directive-28, which established new protections for foreigners' data acquired for foreign intelligence purposes.[173] Even the prospect of facilitated access to U.S.-held data reportedly incentivized the U.K. government to support new judicial review mechanisms—needed in order to be eligible to take advantage of a still-to-be implemented data sharing agreement that would allow U.K. officials to directly compel certain communications content from U.S.-based providers.

But such efforts at extraterritorial rulemaking can also yield conflict, depending on what is being regulated and the relevant interests at stake. Disputes over the right to be forgotten are a case in point. If the CNIL wins the case, it will effectively be imposing its view of what constitutes a legitimate delinking request globally (assuming Google complies). Conversely, if CNIL loses, it will be unable to fully vindicate what it deems a key right. Instead, the United States—via the decisions made by Google—will be imposing its view of how the public's right to know should be implemented in the EU.

---

173. Press Release, Office of the Press Sec'y, Presidential Policy Directive—Signals Intelligence Activities (PPD-28) (Jan. 17, 2014), https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/8HGM-EJZ6].

U.S. requirements that foreign governments meet U.S. standards in order to access U.S.-held communications content are likewise causing direct conflict with key foreign partners. These requirements are seen by key partners as an imperialistic effort to impose the U.S. standard of a warrant based on probable cause, even on foreign states trying to access their own citizens' data in the investigation of local crime. And like other types of unilateral extraterritorial rulemaking, the requirements that foreign governments follow U.S. rules are inherently antidemocratic.[174] They also generate direct conflict of laws when foreign states insist that providers disclose the very same data that U.S. law prohibits them from turning over.

In some subset of cases, such clashes may help to bring two or more states to the table to work out their differences directly. This is an example of unilateral global rulemaking leading to bilateral or multilateral consensus building. The United States and United Kingdom, for example, were incentivized to devise a new scheme for law enforcement access to data because, in part, there was a direct conflict between U.K. and U.S. law—with U.K. law permitting extraterritorial jurisdiction over stored communications content and U.S. law prohibiting providers from directly disclosing U.S.-held data. Broad assertions of law enforcement jurisdiction by the Belgians that at times have conflicted with other states' laws have helped put the issue of law enforcement jurisdiction high on the EU's agenda. Similarly, EU privacy regulations, which require compliance with a long list of requirements before companies can transfer a range of data from the EU to the U.S., have brought EU and U.S. negotiators together and led to some modest changes in U.S. law—all in an effort to protect the ability of companies to transfer data across borders.

Whether or not such unilateral global rulemaking is normatively desirable depends significantly on what is being regulated and how. My point here is not to take a normative stand. My goal here is simply to highlight—joining many others that have done so before me—the increasing possibility and reality of territorial regulation and rulemaking with broad extraterritorial effect. Thus, while the unterritorialists' vision of new supranational institutions and internet governance has not come to pass, there is a new form of global rulemaking and regulation being carried out via local regulation and law. It operates via the unilateral exercise of authority by one state

174. For some, this makes any such effort at unilateral global rulemaking suspect. *See, e.g.*, Parrish, *supra* note 12, at 856–74. My view is that the verdict is more mixed—although my goal here is merely to examine the various implications rather than take a normative stand.

combined with market forces and the multinational nature of the actors being regulated. When effective, it can lead to harmonization of practices across borders and, perhaps, increased protections for all. When ineffective, however, it can yield a potentially destabilizing clash of norms and legal obligations—pushing practices in a direction that contradicts a state's own norms and values.

Moreover, multinational corporations, rather than governments, are often the key players in determining whose rules gain dominance and how. I turn to the implications of that reality now.

C. Role of the Private Sector

As this discussion highlights, such forms of unilateral, global rulemaking are mediated through private sector actors rather than states or international institutions, making the private sector a central player in deciding whose rules apply and thus the scope of privacy and speech rights on a global scale. When Mark Zuckerberg compared Facebook to a government, he was not exaggerating.[175] But it is a government that is neither democratically elected nor democratically accountable, at least in the traditional way of individuals going to the voting booth and choosing or rejecting particular candidates. A range of private decisions, including where to locate data, where to locate personnel, how to structure technology, when to fight and when to comply with government demands, and whether to enter (or pull out of) a particular market, all determine the security of our data and set privacy and speech rights on a global scale. This in turn has profound implications for the possibility of democratic accountability, highlighting the need for alternative forms of accountability and oversight of the private institutions that wield so much power.

The fight over and implementation of the right to be forgotten provides one particularly notable example of the power being wielded by the private sector. In deciding to fight the request, Google sought to impose *its* vision of what is and is not a legitimate takedown request. (Presumably Google also thought a high-profile fight—and win—would protect them from other attempts at government censorship.) It could, however, have simply chosen to quietly comply—and the fact of both the request and Google's compliance likely would never have been publicly known. It could, in fact, still change its approach and decide to delist all of the data from the google.com site, without in any way running afoul of U.S. or other legal obligations.

175. *See* FOER, *supra* note 6, at 61.

Meanwhile, as Google seeks to implement the right to be forgotten, it is doing so with minimal oversight. In fact, the ECJ ruling effectively dictated this result when it placed the initial obligation to delist on Google, rather than some public or quasi-public body. Google's decisions have no precedential value and are not published anywhere. And while a data subject can complain to a government entity—the Data Protection Authority, for example—that his or her request is denied, there does not appear to be any mechanism for a member of the general public to either know about a decision to delink information or object to such a decision.[176]

The dispute over the right to be forgotten is just one of many examples of major multinational companies battling the government and shaping the rules in the process.[177] Lawsuits by Microsoft over gag orders issued in conjunction with search warrants,[178] by Apple over decryption orders,[179] and by Yahoo! over the scope of foreign intelligence surveillance[180] all offer additional examples of company decisions to protest that have led to significant changes in surveillance policy. The *Microsoft Ireland* case is yet another.[181] But nothing compelled the private sector to fight in any of these cases. They did so for a combination of normative and business reasons. Challenging the U.S. government is good for corporate image and thus good for business, particularly in the wake of the Edward Snowden revelations.

But just as there are a handful of instances in which the corporations have chosen to fight, there are countless others where companies have willingly cooperated. With the simple decision to comply or resist law enforcement (and other) demands for data, these companies play an enormous role in setting the scope of privacy and speech rights on a global or near-global scale. After all, the five biggest U.S. tech companies, for example, receive well over one hundred

176. Notably, Brazil's highest court for nonconstitutional questions, the Superior Court of Justice, recently rejected the right to be forgotten precisely because of the concern as to how much power would be delegated to private decisionmakers. According to the Brazilian court, such private-sector adjudication of the right turns search engines into "digital censors." *See* Glyn Moody, *Senior Brazilian Court Says "Right to Be Forgotten" Cannot Be Imposed on Search Engines*, TECHDIRT (Nov. 29, 2016, 3:25 AM), https://www.techdirt.com/articles/20161123/09244936123/senior-brazilian-court-says-right-to-be-forgotten-cannot-be-imposed-search-engines.shtml [https://perma.cc/X3T5-XJVC].

177. *See* Alan Z. Rozenshtein, *Surveillance Intermediaries*, 70 STAN. L. REV. (forthcoming 2018) (analyzing how companies such as Facebook, Apple, and Google function as surveillance intermediaries to constrain government surveillance).

178. Microsoft Corp. v. U.S. Dep't of Justice, 233 F. Supp. 3d 887 (W.D. Wash. 2017).

179. Clark D. Cunningham, *Apple and the American Revolution: Remembering Why We Have the Fourth Amendment*, 126 YALE L.J. FORUM 216, 216–17 (2016).

180. *In re* Directives [redacted text] Pursuant to Section 105B of the Foreign Intelligence Surveillance Act, 551 F.3d 1004 (FISA Ct. Rev. 2008).

181. *See* discussion *supra* Section I.A.1.

thousand requests every six months for such information from governments all around the world.[182] Combined, they produce data in response to approximately fifty to seventy-five percent of those requests. In so doing, they are independently deciding what standards to apply in evaluating the requests, what requests meet those standards, and how much information should be provided in response.[183]

In other situations, companies are effectively forced into choosing whose law to favor. Consider, for example, the conflict of laws caused by one state asserting broad extraterritorial jurisdiction to compel the production of data located in another state's territory and countervailing blocking provisions prohibiting disclosure in the state where the data is found. The provider then has to decide: Whose law should I violate and whose should I comply with? A number of practical considerations are likely to dictate the result: With which state does the provider have stronger ties and greater business interests? What is the penalty of noncompliance? The decision is of course shaped by the relative coercive powers of the states. But it is ultimately a decision for the private corporation.

* * *

The amount of power wielded by major multinational corporations has profound implications for how one thinks about promoting data security and safeguarding privacy and speech rights. Governments are no longer the primary, or in some cases even the central, actor. Their role is both supplemented and sometimes supplanted by the private actors that manage our data and mediate conflicting legal obligations across borders. Moreover, in many cases governments are no longer operating in direct interaction with their

182. *See, e.g., Law Enforcement Requests Report*, MICROSOFT, https://www.microsoft.com/about/csr/transparencyhub/lerr/ (last visited Oct. 20, 2017) [https://perma.cc/VEM4-4L79] (select "2016 (Jul-Dec)" filter); *Report on Government Information Requests: January 1 - June 30, 2016*, APPLE, http://images.apple.com/legal/privacy/transparency/requests-2016-H1-en.pdf (last visited Oct. 20, 2017) [https://perma.cc/883E-QAYV]; *Transparency Report: Government Data Requests*, YAHOO!, https://transparency.yahoo.com/government-data-requests/index.htm (last visited Oct. 20, 2017) [https://perma.cc/8JLU-SY2N]; *Transparency Report: Requests for User Information*, GOOGLE, http://www.google.com/transparencyreport/userdatarequests/ countries/?p=2016-06 (last visited Oct. 20, 2017) [https://perma.cc/NER8-EG3B].

183. In fact, frustration over the lack of clarity and consistency across providers as to how these decisions are being made has resulted in an EC-led initiative to engage in standard-setting with respect to the disclosure of such subscriber information. *See* EUR. COMM'N REPORT, *supra* note 62, at 7 (disclosure determinations "regulated only through individual company policy on the provider side, [are] not predictable and thus not reliable for either side").

citizenry. Governmental searches, seizures, and takedown requests are increasingly directed at private, third-party providers, rather than directly targeted at the individual object of a search, seizure, or takedown request. This suggests the need for new types of accountability measures focused on the powerful private actors that manage so much of our data. Here, I very briefly suggest three, although this is just the beginning of the conversation; it is an area that requires much more thought and analysis than is possible here.

First, mandatory and detailed transparency reporting requirements are a start. Such reporting helps inform the public and thus allows those individual consumers that do care enough to "vote" by choosing the company that manages their data in a way consistent with their norms and preferences. The effectiveness of such measures depends, of course, on how much the public is willing to scrutinize the reports and make decisions about what products to buy and services to use as a result. But even if only a small subset of the population cares enough to do so, the small subset can have an amplifying effect if it is sufficiently vocal.

Second, public-private partnerships that establish best practices and certify companies that abide by them provide another means of oversight and standard-setting. The Global Network Initiative ("GNI"), launched in 2008, provides a model for what this kind of public-private partnership could look like. It is a multistakeholder initiative involving private companies, civil society groups, academics, and other individuals working together to promote "global digital rights"—including privacy and freedom of expression. By bringing these various actors together, there is the possibility of both establishing best practices and holding the companies involved to account.

In fact, companies that participate in the GNI have consistently been top rated in the annual Ranking Digital Rights 2017 Corporate Accountability Index.[184] The structure is in place for the GNI to play an increasingly active role in standard-setting, although as with all such voluntary compliance measures the efforts are only as good as the incentives for compliance.

Third, increased insistence on notice requirements in a range of different contexts could prove helpful. Notice to users when governments access their data helps ensure that users have some ability to monitor and respond to potentially excessive demands for their information. And while there are often legitimate reasons to *delay*

184. *GNI Companies Again Top Ranking Digital Rights 2017 Corporate Accountability Index*, GLOBAL NETWORK INITIATIVE (Mar. 23, 2017, 12:42), https://www.globalnetworkinitiative.org/news/gni-companies-again-top-ranking-digital-rights-2017-corporate-accountability-index [https://perma.cc/N83E-G9YZ].

notice in order to preserve the integrity of an investigation, there is no sound justification for an *indefinite* refusal or prohibition on such disclosure.

As discussed in the section on remote searches, notice to other governments also can help to ensure transparency about when and for what reasons governments are accessing data of other states' residents and citizens. This information, in turn, can provide the basis for standard-setting across international borders.

Similarly, notice to the producer of information, whenever known, should also be the default rule with respect to takedown requests, albeit again with carve-outs for reasons of national security and privacy.

To be clear, these are initial recommendations meant to spur further conversation. There simply is no one-size-fits-all answer to the question of how to best regulate the private actors that increasingly manage our data and play a role on par with states in setting the scope of privacy and speech rights. Tailored approaches are ultimately needed. These will vary depending on the technology or general matter being regulated, the relative dominance of the respective players, and the applicable incentives. Each of the areas addressed in this Article, for example, requires a slightly different approach—and each deserves its own deep analysis and attention.

My goal here is simply to draw attention to the trends and implications, rather than coming up with anything close to a comprehensive solution. Critically, the key relationships between the government and governed are changing. Speech and privacy rights are increasingly being determined not by government actors, but by large private actors that are accountable not just to a single government, but to many. It is the decisions of these private actors that often determine which government's rules apply, how these rules are interpreted, and how much of our private data is and should be accessible to the governments where they operate.

CONCLUSION

Our data moves across the globe without respect to territorial boundaries. Yet governments continue to assert territorial controls. This raises profound, and still largely unresolved, questions about what is territorial and what is unterritorial, offers the possibility of territorial regulation with broad extraterritorial effect, and puts the multinational companies that manage our data in the position of mediating competing governmental demands and approaches, and ultimately determining the rules. These are powerful trends that require a rethinking of the

enforcement jurisdictional rules that apply and a reassessment of the relationship between the government and the governed. At least with respect to speech and privacy rights, one's own national government may no longer be the most important player; rather, foreign governments and the multinational corporations that manage the disputes across borders are increasingly setting the rules. This in turn requires the development of new forms of accountability for the private actors that are mediating disputes across borders and thus setting privacy and speech rights on a global or near-global scale.