2020

The Overlapping Web of Data, Territoriality and Sovereignty

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

CHAPTER 35

THE OVERLAPPING WEB OF DATA, TERRITORIALITY, AND SOVEREIGNTY

JENNIFER DASKAL*

Sovereignty has long been linked with territoriality. This has been challenged in numerous ways and in numerous contexts over time.[1] But the myth of sovereignty as synonymous with the exclusive and total control over territory remains a central part of how governments conceive of their power, even if increasingly challenged by facts on the ground.

The rise of a globally interconnected internet and, in particular, the ways in which highly mobile data transits and is accessed across state borders poses a particularly profound test to this notion of the sovereign-territoriality link. Data is, after all, both unterritorial and multiterritorial. It can move across territorial boundaries with the speed of light. It does not travel in obvious or observable ways from point A to B; in fact, it sometimes crosses international borders even if the beginning and end points are within the same territorial borders. It can be copied and held in multiple locations at once. It can be remotely accessed by users who are separated by territorial boundaries from the data that they are accessing. And it can be accessed and manipulated by multiple different people—or governmental entities—simultaneously.[2]

* Special thanks to Paul Schiff Berman, Shalev Roisman, participants in the 2017 Global Legal Pluralism Conference, and participants in the 2018 Junior International Scholars Association workshop for their thoughtful comments and critiques.

[1] See, e.g., Stuart Elden, *The Birth of Territory* (Chicago: University of Chicago Press, 2013); Kal Raustiala, *Does the Constitution Follow the Flag? The Evolution of Territoriality in American Law* (New York: Oxford University Press, 2009).

[2] See, e.g., Jennifer Daskal, "Borders and Bits," *Vanderbilt Law Review* 71, no. 1 (2018): 179; Jennifer Daskal, "The Un-Territoriality of Data," *Yale Law Journal* 125 (2015): 325.

These features of data undercut the vision of exclusive, unilateral, state control over things within the state's border. These features also mean that multiple sovereigns may seek to control or access the same piece of data. These interests can sometimes be accommodated. At times, this is a result of harmonization. At times, this is a side benefit of data's divisibility—the feature of data that allows multiple states to access the same data simultaneously without interfering with the ability of others to access it as well.

But the interaction of data with multiple, overlapping jurisdictions generates direct clashes as well. Absent a China-like firewall or more effective geographic filtering than has existed to date, competing visions of speech and privacy rights are yielding increasing and hard-to-resolve conflicts. Absent a means to resolve those disputes, we risk generating a fragmented internet, as states increasingly mandate local storage as a means of ensuring local control.

Importantly, both the harmonization efforts and the clashes that emerge are increasingly managed by major multinational companies that handle so much of the world's data and thus mediate disputes across borders. This has two important consequences. First, it puts private actors, namely, large multinational tech companies, in the driver's seat, often displacing governments as the central players in determining a host of privacy, security, and speech-related issues. Second, it yields the possibility of a new form of international law and norm-making, via territorial regulation with broad extraterritorial reach, as mediated by private actors rather than states coming together to negotiate common rules and norms.

In this chapter, I examine these trends through three different examples: law enforcement efforts to access data across borders, state-based content regulation, and privacy-based regulations as an effort by states to assert sovereign control. These are hardly the only areas in which data is putting pressure on the territorial-sovereign link and yielding new efforts at control. But together they illustrate some of the key issues and challenges. In examining these issues, I make four broad key claims:

First, despite the predictions and hopes of some, the rise of an interconnected global internet has failed to yield a new form of supranational governance.[3] To the contrary, states have and continue to impose territorial-based regulations and controls on the data that flows through and is accessed by the residents in their states. The recent trend in favor of data localization mandates—pursuant to which companies operating in a jurisdiction must store specific categories of data locally—provide a powerful example of sovereign states seeking to reassert territorial-based controls.[4]

[3] See, e.g., David R. Johnson and David G. Post, "Law and Borders—The Rise of Law in Cyberspace," *Stanford Law Review* 48 (1996): 1367; John Perry Barlow, "A Declaration of the Independence of Cyberspace," *Electronic Frontier Foundation*, Feb. 8, 1996, http://homes.eff.org/~barlow/Declaration-Final.html [https://perma.cc/W4QE-J73B].

[4] See, e.g., Jennifer Daskal & Justin Sherman, *Data Nationalism on the Rise,* Catalyst Working Power (forthcoming 2020); Robert Morgus, Jocelyn Woolbright, and Justin Sherman, *The Digital Deciders: How a group of often overlooked countries could hold the keys to the future of the global internet* (Washington, D.C.: New America, October 23, 2018), https://www.newamerica.org/cybersecurity-initiative/reports/

Second, as states seek to assert territorial-based controls, what is territorial and what is extraterritorial remains in sharp dispute. This is particularly acute with respect to debates over law enforcement access to data, but has resonance in other areas as well.[5] The question as to the proper scope of territorial-based regulation, particularly with respect to content-based regulations, is an increasingly potent source of dispute.

Third, territorial-based regulation with broad extraterritorial reach exemplifies a new form of international lawmaking but via unilateral, state-based decision-making, as mediated by private actors, rather than either new treaties or the generation of new rules by new supranational institutions[6]. This generates both promise and challenges. Rights-respecting states, for example, can use their market power to impose regulatory structures that promote privacy and personal security, among other norms, with broad, extraterritorial reach. Rights-destructive states can do the same.

Fourth, and relatedly, many of the fundamental privacy, security, and speech-related questions raised by the management of data are being either implicitly or explicitly delegated to multinational companies that manage data across borders. When Mark Zuckerberg, the CEO and founder of Facebook described his company as akin to a government, he wasn't exaggerating.[7] Everything—from where it houses its employees and stores its customers' data, how it designs its products, and what data it retains and for how long—has an enormous effect on speech and privacy rights as well as the relative power of particular states to control.[8] This changes the relationship between governments and the governed and the prospects for democratic accountability, adding in a dynamic power source that requires new theories of accountability and control.

The remainder of this chapter proceeds in two key parts. It first examines these challenges in the specific contexts of law enforcement efforts to access data across borders, state-based content regulation, and privacy-based controls. It then teases out key implications for security, privacy, and speech rights, the future of international law-making, the power of the state, and the need for new forms of accountability and control.

digital-deciders/. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?," *Information Technology & Innovation Foundation* (May 2017): 13–17, https://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.65050406.927448598.1504895329–310094596.1504895329[https://perma.cc/C257-P7UF].

[5] See, e.g., Cybercrime Convention Committee (T-CY), "Criminal Justice Access to Electronic Evidence in the Cloud: Recommendations for Consideration by the T-CY," *Council of Europe* (Sept. 16, 2016): 7–8, http://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=0900001680a495e [https://perma.cc/N6TK-QVXE]. The T-CY describes the array of jurisdictional challenges that are arising in connection with attempts to regulate data and the myriad of different state responses.

[6] *See* Jennifer Daskal, *Speech Across Borders,* 105 Va, L, Rev, *1605 (2019)* https://www.virginialawreview.org/sites/virginialawreview.org/files/Daskal_Book.pdf.

[7] See Franklin Foer, *World Without Mind: The Existential Threat of Big Tech* (New York: Penguin Press, 2017), 61.

[8] See, e.g., Alan Z. Rozenshtein, "Surveillance Intermediaries," *Stanford Law Review* 70 (Jan. 2018): 99.

35.1 Data's Challenges

The rise of the global internet yielded early predictions of new supranational institutions that would manage the world's data.[9] But this newfound universalism never came to pass. To the contrary, states found a variety of ways to assert territorial-based controls over data and the people and companies that managed the data that flowed through their countries.

That said, the assumption that territorial-based controls would ensure democratic accountability over data and the rules governing that data also turned out to be a faulty hope as well.[10] Rather, we have seen the rising power of new multinational and non-democratically accountable corporations that manage the world's data. It is a classic example of what Professor Paul Schiff Berman has labeled "legal pluralism"—with multiple different and overlapping actors setting the rules.[11] And it has yielded a number of still unresolved questions about the permissible reach of state regulation and control, including fundamental questions about what is territorial and what is extraterritorial, the scope of the state's authority over extraterritorially located or accessed data, and the possibility—or not—of new mechanisms of accountability and control.

The following examines how these issues are playing out in three discrete areas: law enforcement access to data across borders, content regulation with broad extraterritorial reach, and data transfer restrictions as a means of enforcing territorial-based controls. The discussion focuses in particular on the implications for security, privacy, and speech rights—as these are the issues most directly implicated by these three areas of inquiry.

35.1.1 Law Enforcement Access to Data Across Borders

The question of how far law enforcement reaches data held outside its territorial borders is being debated in the halls of Congress and various capitols around the world, was the basis for a lawsuit that went all the way to U.S. Supreme Court, and is the subject of legislative reform efforts across the globe. I use the now-resolved *Microsoft Ireland* litigation in the United States to frame the issues and then turn to some of the other reform efforts that has ensued.

[9] See, e.g., Johnson and Post, "Law and Borders—the Rise of Law in Cyberspace," *supra* note 4, at 1367.

[10] See, e.g., Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World* (New York: Oxford University Press, 2006). Goldsmith and Wu predict territorial-based controls and celebrate the result as a victory for the principle of democratic accountability.

[11] See, e.g., Paul Schiff Berman, *Global Legal Pluralism: A Jurisprudence of Law Beyond Borders* (New York: Cambridge University Press, 2012); Paul Schiff Berman, "Global Legal Pluralism," *Southern California Law Review* 80 (2007): 1155.

35.1.1.1 *The Microsoft Ireland Case*

The *Microsoft Ireland* case dates to December 2013, when the U.S. government served a warrant on Microsoft, seeking access to emails associated with a suspect in a drug case.[12] Microsoft refused to comply, on the grounds that the data was located in Dublin, Ireland, and thus outside the territorial borders of the United States. According to Microsoft, U.S. law enforcement only had jurisdiction over data physically located in the United States. The U.S. government, by contrast, argued that since Microsoft employees could access the data from within the United States, it had jurisdiction to compel. According to the government, what mattered was the location of Microsoft employees, not the location of the data; it could use its warrant authority to compel Microsoft, a U.S.-based company, to turn over data irrespective of where the data is located.[13]

The case raised key questions about how territorially limited law enforcement authorities map onto data and the multinational corporations that control the data. It is, after all, a long-standing premise of international law that law enforcement agents in State A cannot unilaterally enter State B and seize property, absent State B's consent—a principle that has also been enshrined in U.S. law.[14] Doing so would be a violation of State B's sovereignty—based on an understanding of sovereignty as providing an exclusive monopoly on law enforcement actions within a state's own territorial borders.

But that understanding fails to answer the key issues presented by the globally interconnected data managed by large private companies that operate across the globe: what is territorial and what is extraterritorial? Do the location of the 0s and 1s being sought determine sovereign interests and control? The location of the company that controls the 0s and 1s? Or something new altogether?

As I have argued elsewhere, the position that location of data controls—the position taken by Microsoft in the case—is a troubling one.[15] It generates a range of concerning

[12] See Microsoft Corp. v. United States, 829 F.3d 197, 200 (2d Cir. 2016), *reh'g denied*, 855 F.3d 53 (2d Cir. 2017) (en banc).

[13] The magistrate and district court judge sided with the government, but the Second Circuit reversed, ruling in favor of Microsoft. See *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 15 F. Supp. 3d 466, 477 (S.D.N.Y. 2014); *In re* Warrant to Search a Certain E-Mail Account Controlled and Maintained by Microsoft Corp., 829 F.3d 197, 222 (2016). The U.S. Supreme Court agreed to hear the case and oral arguments took place in February 2018. See, e.g., Jennifer Daskal, "Microsoft Ireland Argument Analysis: Data, Territoriality, and the Best Way Forward," *Harvard Law Review* (blog), Feb. 28, 2018, https://blog.harvardlawreview.org/microsoft-ireland-argument-analysis-data-territoriality-and-the-best-way-forward/ [https://perma.cc/6R6Q-ZBQR]. The case was mooted by the passage of legislation before the U.S. Supreme Court ruled.

[14] See, e.g., Restatement (Fourth) of the Foreign Relations Law of the United States § 402(b) & Notes 3 (2018); Fed. R. Crim. Pro. 41(b). The Federal Rule establishes that warrant jurisdiction is territorially limited, albeit with a few limited exceptions allowing warrants to reach to U.S. territories and diplomatic outposts.

[15] See, e.g., Daskal, "Borders and Bits," *supra* note 3, at 221–26. Even Microsoft recognizes that rules that delimit jurisdiction based on data location fail to serve the critical privacy, security, and sovereignty interests at stake, and in fact the company supports a reform of the underlying legislation. Microsoft nonetheless argues that this is a decision for Congress—and that a proper read of the current statute does in fact impose these location-based limitations on jurisdiction that it agrees should be

policy implications, including the incentivization of mandatory data localization mandates, pursuant to which companies must store some or all data locally, as a means of ensuring law enforcement access. This has efficiency, security, and privacy costs. It potentially prices small start-ups out of the international market, given the high cost of complying with these laws. It can lessen security if companies are forced to host data in local, but less secure, environments. And it is employed by repressive states as a means of keeping tabs on dissidents, human rights activists, and others that express views contrary to that of the government's.

Such a rule also significantly undercuts the state's legitimate interests in, and ability to, prosecute and prevent future crime. It delegates to private parties the power to place data in—or out of—a requesting state's jurisdiction. These private party determinations are often based on a range of factors, such as tax and energy costs, efficiency, and latency time, that have nothing to do with the security, privacy, or other related interests at stake. In many cases, the host state may have absolutely no connection to the data, the people with a possessory interest in the data, or any other aspect of the crime being investigated; the only connection may be that a third-party provider decided to house it there.

In some cases, there may not even be any government with jurisdiction over both the people that can access the data and the data being sought—meaning that the requesting government can neither access the data directly nor turn to a foreign partner for help.[16] In other words, there may be *no* way to compel access, no matter how great the need, or how robust the substantive and procedural protections adhered to by the requesting state.

Moreover, such a rule threatens to yield a reduction in privacy benefits for those subjects to particular demands for data, at least in certain circumstances. Consider, for example, the U.S. requirement of a warrant, issued by an independent judge or magistrate, based on a finding of probable case. Rather than obtaining a warrant pursuant to these standards, American law enforcement is told to work through foreign governments to access sought-after data, employing the procedural and substantive rules in

amended. See, e.g., *Facilitating Cooperation and Protecting Rights: Hearing on Law Enforcement Access to Data Stored Across Borders Before the Subcomm. On Crime and Terrorism of the S. Comm. on the Judiciary*, 115th Cong. (2017) (statement of Brad Smith), https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20Smith%20Testimony.PDF [https://perma.cc/3H3F-XCN2]. Smith emphasized that "litigation is not a substitute for policymaking" and urged Congress to update the Electronic Communications Privacy Act. Brief in Opposition to Petitioner for a Writ of Certiorari, *In re* Warrant to Search Certain E-Mail Account Controlled and Maintained by Microsoft at 3, No. 17–2 (Sup. Ct. Aug. 28, 2017) (suggesting that Congress should "craft a new legislative scheme for a world not anticipated in 1986"). The judge who authored the Second Circuit opinion likewise urged an amendment of the statute to better reflect the underlying interests at stake. See *In re* Warrant to Search Certain E-Mail, 855 F.3d at 55 (Carney, J., concurring) (urging Congress to act).

[16] See, e.g., *In re* Search Warrant No. 16-960-M-01, 2017 U.S. Dist. LEXIS at *37–38 (warning that there would be no alternative means for the government to access certain data held by Google); Petition for Rehearing and Rehearing En Banc, Microsoft v. United States, No. 14–2985, at 17–19 (2d Cir. Oct. 13, 2016).

place in whatever jurisdiction where the data happens to be located.[17] In many cases, these standards will be *less* privacy protective than U.S.-based warrant requirements.

On the other hand, a system in which the government can compel production of any and all data so long as it can claim jurisdiction over the providers that manage data yields troubling implications as well. It sets a concerning precedent unmoored from any baseline privacy protections or other relevant considerations such as the legitimacy of the government's claimed need for the data. The United States is, after all, not the only government asserting such broad jurisdictional claims over providers in its jurisdiction. Others have gone even further—arguing that they can compel production from any provider that offers services oriented to its residents, even if the relevant provider is not physically located in the requesting country's territory.[18] These kind of broad claims, if adopted widely and without appropriate safeguards, threaten a race to the bottom, with states all over the world compelling access to data based on their own, often weakly protective, rules governing access. It also means that individuals will have little knowledge of who is accessing their data and for what reasons—let alone any ability to seek accountability or respond to either abuse or mistake.

Such a rule also fails to respect the legitimate sovereign interests in protecting the interests—and thus setting the rules with respect to privacy, associational, and speech rights—of one's own citizens and residents. Principles of democratic accountability further highlight the concerns with a system in which foreign governments can unilaterally compel data of anyone, anywhere, without regard to their location, nationality, or relevant connections to the requesting state. Citizens and residents have, at least in theory, some say over the policies and practices of their own states; they have little to no say in the policies and practices of foreign sovereigns.

In addition, such broad assertions of jurisdiciton generate increasingly potent conflict of laws, with some states compelling production over the same data that other states prohibit from being turned over, as addressed in what follows.[19]

[17] The relevant U.S. statute, the Stored Communications Act, authorizes the U.S. government to compel communications content based on a standard less stringent than a warrant issued based on a finding of probable cause in certain circumstances. See 18 U.S.C. § 2703 (2012). But the Sixth Circuit has, as a matter of constitutional law, required a warrant anytime the U.S. government compels the production of emails. See U.S. v. Warshak, 631 F. 3d 266, 288 (6th Cir. 2010) (holding that "[t]he government may not compel a commercial ISP to turn over the contents of a subscriber's emails without first obtaining a warrant based on probable cause"). The U.S. government now treats that decision as binding on a national basis and seeks a warrant anytime it seeks to compel production of communications content from a service provider. And both the reasoning of and dicta in the Supreme Court's decision in *U.S. v. Carpenter*, 138 U.S. 2206 (2018), indicates that this is now required as a constitutional rule.

[18] Procureur-Général v. Skype, Correctionele Rechtbanken [Criminal Tribunal] Antwerp, Division Mechelen, Oct. 27, 2016, No. ME20.4.1 105151–12, ¶¶ 1.2–1.5 (Belg.); Hof van Beroep [Court of Appeal] Antwerpen, 12e ch. Nov. 20, 2013, 2012/CO/1054 (Belg.) (translated in *Digital Evidence & Electronic Signature Law Review* 11 (2014): 137, http://sas-space.sas.ac.uk/5720/1/2138-3141-1-SM.pdf [https://perma.cc/84YR-REMR]); Paul de Hert and Monika Kopcheva, "International Mutual Legal Assistance in Criminal Law Made Redundant: A Comment on the Belgian Yahoo! Case," *Computer Law & Security Review* 27 (2011): 291–92.

[19] See Jennifer Daskal, "Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues," *Journal of National Security Law & Policy* 8 (2016): 473.

35.1.1.2 *Challenges Posed by Blocking Statutes*

So-called "blocking statutes" prohibit companies from transferring data to foreign governments, including requesting law enforcement officials, in a range of situations. Of particular global import, the same U.S. law at issue in the *Microsoft Ireland* case prohibits U.S.-based companies from turning over U.S.-held stored communications content directly to foreign governments.[20] This has become an increasing source of frustration for governments due to a combination of three key facts. First, the evolving internet infrastructure and growth of the so-called cloud means that data relating to a government's own citizens is increasingly stored outside the home government's territorial jurisdiction. Second, the dominance of U.S.-based providers means that a significant portion of that data is U.S.-held. And third, the rising use of encryption means that access to the stored content is increasingly the only way for governments to access content of interest.[21] Even a few years ago, foreign governments could access data transiting their territory, even if they were unable to access content when it was stored. But the default use of encryption with respect to data in motion makes it impossible, or at least very difficult, to decipher data crossing local communications channels.

Due to these U.S. blocking provisions, foreign governments seeking U.S.-held data make a diplomatic request for such data, employing what is known as the mutual legal assistance (MLA) process. Use of the MLA system a time-consuming and multilayered process that requires multiple reviews by the U.S. Department of Justice, a U.S. attorney to obtain a warrant for the data on behalf of the foreign government, and application of the U.S. standard of probable cause—a standard that is unfamiliar to many foreign governments.[22] The use of the MLA system is required even when foreign governments are investigating their own citizens in the commission of local crime, and the only U.S. nexus is that the target uses a U.S.-based provider and the data happens to be U.S.-held.

Many other countries have similar, and even broader, blocking provisions in place than those of the United States—covering non-content data as well as communications content.[23] The European Union's General Data Protection Regulation (GDPR), for example, prohibits transfer of the personal data of EU residents outside of the European

[20] See 18 U.S.C. § § 2701 et seq.

[21] See, e.g., Peter Swire, "Why Cross-Border Requests for Data are Becoming More Important," *Lawfare* (blog), May 23, 2017., https://www.lawfareblog.com/why-cross-border-government-requests-data-will-keep-becoming-more-important

[22] 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," *The White House: President Barack Obama* (Dec. 12, 2013), 227–28. The report noted that it takes an average of ten months for the United States to process the Mutual Legal Assistance Treaty (MLAT) requests. See also Jonah Force Hill, "Problematic Alternatives: MLAT Reform for the Digital Age," *Harvard National Security Journal* (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age [https://perma.cc/2GMD-Q29X]. Hill noted that it often takes months, if not years, for foreign governments to respond to MLAT requests.

[23] See Commission Services, "Progress Report Following the Conclusions of the Council of the European Union on Improving Criminal Justice in Cyberspace," *Council of the European Union* (Dec. 2, 2016), 6, http://data.consilium.europa.eu/doc/document/ST-15072-2016-INIT/en/pdf [https://perma.cc/9GME-9L5Z] [hereinafter European Commission Report].

Union unless pursuant to specific exemptions, such as an explicit international agreement.[24] There is an open question as to whether, and in what situations, providers are permitted to turn over EU-held data in response to lawfully-issued compelled disclosure orders issues by foreign law enforcement officials.[25]

35.1.1.3 *Legislative Responses*

The United States' Clarifying Lawful Overseas Use of Data (CLOUD) Act, draft EU e-Evidence proposals, and draft updates to the Council of Europe's Budapest Convention all seek better align the jurisdictional rules with the key sovereign interests at stake.[26]

The CLOUD Act, for example, addresses both the issue presented to the Supreme Court in the *Microsoft Ireland* case (thereby mooting the case) and the converse issue of foreign governments seeking U.S.-held content.[27] Specifically, it authorizes the U.S. government to compel production of communications content without regard to the location of the data. At the same time, it establishes a new statutory mechanism for providers to move to quash based on comity grounds, albeit in limited situations. In adjudicating these comity claims, courts are directed to consider, among other factors, the location and nationality of the target, the importance of the evidence to the investigation, and the possibility of obtaining sought-after data through alternative means—all factors that map better onto the key interests at stake than where the data happens to be located.[28] The legislation also explicitly notes the availability of common law comity claims in those situations in which the statutory comity claims are not available.[29]

[24] GDPR, 2016 O.J. (L 119) 1, art. 48.

[25] See Brief of the European Commission on Behalf of the European Union as Amicus Curiae in Support of Neither Party, Microsoft v. Ireland, No. 17–2, at 14–15 (Sup. Ct. 2018) (noting that "a foreign court order does not, as such, make a transfer lawful under the GDPR," but suggesting that certain exceptions on the transfer prohibitions might apply). Separately, there are agreements in place 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* (Aug. 9, 2015), 4, https://perma.cc/9887-7M24; European Commission, "Questions and Answers on the E.U.-U.S. Data Protection 'Umbrella Agreement,'" Dec. 1, 2016, http://europa.eu/rapid/press-release_MEMO-16-4183_en.htm [https://perma.cc/U6S6-WNTR]. The press release discussed the intent to facilitate data transfer between the European Union and the 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."

[26] See, e.g., Clarifying Lawful Overseas Use of Data (CLOUD) Act, Pub. L. No. 115-141, 132 Stat. 348 (2018); *Proposal for a Regulation of the European Parliament and of the Council on European Production and Preservation Orders for Electronic Evidence in Criminal Matters*, 15010/18 (Nov. 30, 2018), http://data.consilium.europa.eu/doc/document/ST-15020-2018-INIT/en/pdf [https://perma.cc/L8KK-KMLA]; Towards a Protocol on Evidence in the Cloud," Council of Europe, June 8, 2017, https://www.coe.int/en/web/cybercrime/-/cybercrime-towards-a-protocol-on-evidence-in-the-cloud [https://perma.cc/86U9-RKA2].

[27] The CLOUD Act, S. 2383, 115th Cong. (2018).

[28] CLOUD Act § 103(a)–(b) (to be codified at 18 U.S.C. §§ 2703(b), 2713). Providers can bring such claims if the foreign government is seeking the data of a non-U.S. citizen or resident located outside the United States and the request generates a conflict of laws with a country subject to an executive agreement on cross-border data sharing with the United States.

[29] CLOUD Act § 103(c).

The CLOUD Act also authorizes the executive branch to enter into executive agreements with foreign governments, pursuant to numerous conditions, designed to facilitate the cross-border access to communications content.[30] Partner governments can directly request communications content from U.S.-based providers if they are seeking the data of foreigners outside the United States in the investigation of serious crime, and if the requests comply with a range of baseline substantive and procedural protections. If, however, the partner government is seeking the data of U.S. citizens or legal permanent residents, or anyone else physically in the United States, it needs to work through the mutual legal assistance process. In such situations, U.S. officials have to obtain the data, pursuant to a warrant based on probable cause, on behalf of the foreign government. The partner government also must ensure the United States the reciprocal ability to compel data from foreign-based providers.

Importantly, the legislation sets a number of parameters on how these executive agreements operate. Partner governments must first be certified as affording "robust substantive and procedural protections for privacy and civil liberties."[31] More importantly, each request must be particularized, targeted, and either reviewed or overseen by a judge or other independent entity. Additional protections are in place to ensure that irrelevant data is deleted and to protect against the system being used to pass information back and forth between the two governments in an end run around rules governing domestic access that would normally apply. Importantly, the legislation also requires that the partner government subject itself to compliance reviews by the United States. The agreements also sunset after five years unless renewed.[32]

This approach reflects a sensible shift in focus away from the location of data to the location and nationality of the targets of the investigation. It gives governmnets the key tools to investigate and prosecute local crime—without regard to the location of the data.—while also ensuring that governments can continue to set the rules with respect to the direct accessing of theirown citizens and residents. And, importantly, it does so in ways that sets baseline protections governing the specific requests that are made.

Meanwhile, the European Union is actively considering a new e-Evidence Regulation that would facilitate law enforcement access to data across borders and lay out a set of baseline rules that would govern access to data by European governments.[33] The Council of Europe is considering a similar set of issues with respect to non-content data.[34]

[30] Ibid., § 105(a) (codified at 18 U.S.C. § 2523). [31] Ibid.

[32] Ibid. For a further elaboration of these protections, see Jennifer Daskal, "*Microsoft Ireland*, the CLOUD Act, and International Lawmaking 2.0," 71 *Stanford Law Review Online* 9, 13–15 (2018), https://www.stanfordlawreview.org/online/microsoft-ireland-cloud-act-international-lawmaking-2-0 [https://perma.cc/T763-VX69]; Jennifer Daskal and Peter Swire, *Why the CLOUD Act Is Good for Privacy and Human Rights*, *Just Security* (Mar. 14, 2018), https://www.justsecurity.org/53847/cloud-act-good-privacy-human-rights [https://perma.cc/79Z7-NCKV].

[33] *See* Theodore Christakis, *E-evidence in a Nutshell*, Cross Border Data Forum (Jan. 14, 2019), https://www.crossborderdataforum.org/e-evidence-in-a-nutshell-developments-in-2018-relations-with-the-cloud-act-and-the-bumpy-road-ahead/.

[34] *See* Cybercrime Convention Committee, (Draft) Terms of Reference for the Preparation of a 2d Additional Protocol on the Convention on Cybercrime (June 1, 2017), [https://perma.cc/PWD3-PESH].

35.1.2 Content Restrictions

Efforts to control content highlight the power of territorial regulation with broad, extra-territorial effect and the power of multinational companies to mediate the disputes that emerge. The ongoing dispute over the territorial reach of Europe's right to be forgotten—now before the European Court of Justice (ECJ)—provides a notable example. This is a follow-on case from an earlier ECJ decision affirming the right of individual users to demand that search engines de-index personal information about the user.[35] According to the ECJ, the right applies even if the information is true. It does not even require a finding of prejudice. Rather the data subject need only establish that the information 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," and the search engine is required to delink it—absent a determination that the data subject is a "public figure" and there is a countervailing public right to know.[36]

The ECJ, however, 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—the search engine of choice for about 90 percent of EU residents[37]—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 Party—a powerful group of Data Protection Officers from across the European Union—deemed this 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.[38]

In May 2015, the French data protection agency (CNIL) took up the mantle and ordered Google to remove delinked information from all applicable domains, including the.com

[35] See Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos (AEPD), May 13, 2014, http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&docid=152065&cid=244711 [https://perma.cc/EXN3-9XJX].

[36] Ibid., ¶¶ 4, 82, 94.

[37] The rest of the market is split primarily between Bing (owned by Microsoft), Yahoo!, and Baidu (a Chinese-based search engine). See "Search Engine Market Share," *NetMarketShare*, https://www.netmarketshare.com/search-engine-market-share.aspx?qprid=4&qpcustomd=0 [https://perma.cc/JFD7-KN2D] (last accessed Aug. 2017).

[38] See Article 29 Data Protection Working Party, "Guidelines on The Implementation of the Court of Justice of the European Union Judgment on 'Google Spain and Inc. v. Agencia Espanola de Proteccion de Datos (AEPD) and Mario Costeja Gonzalez' " C-131/12 6, Nov. 26, 2014, https://www.pdpjournals.com/docs/88502.pdf [https://perma.cc/6KUE-PAU8].

domain.[39] After a series of court battles, Google agreed to make relevant information inaccessible to anyone accessing the search from within the European Union. But it continued to make the information available to others who access Google's search from outside the European Union.

But for the CNIL, this didn't go far enough. The CNIL insisted that the right to be forgotten, which it deems a fundamental right, will not be protected absent global de-indexing—a delinking of the offending link across all of Google's sites everywhere.

Google, conversely, argued that it is willing to abide by the requirements of the right to be forgotten in the European Union, but that the European Union should not be imposing its particular vision of speech and privacy rights on the rest of the world. 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 demanding that their laws regulating information likewise have global reach?"[40] Walker warned 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.[41] Google further argued that its current approach is effective in protecting the applicable right, given that 97 percent of French users access the search engine via Google.fr. While not foolproof, the vast majority of French users would not see the link.[42]

In a September 2019 ruling, the ECJ concluded that EU law did not give the French data protection agency the authority to compel global takedowns. But it left open the possibility that France or other EU states could continue to mandate such global takedowns as a matter of domestic, rathern than EU law.[43] And in a subsequent ruling in a

[39] 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."

[40] Alex Hern, "Google Takes Right to Be Forgotten Battle to France's Highest Court," *Guardian*, May 19, 2016, https://perma.cc/A4H3-7C5H.

[41] Ibid.

[42] Carol A.F. Umhoefer and Caroline Chance, "Right to Be Forgotten: The CNIL Rejects Google Inc.'s Appeal Against Cease and Desist Order," *Privacy Matters* (blog), *DLA Piper*, Sept. 22, 2015.

[43] See Judgment of the Court, Google v. Commission nationale de l'informatique et des libertés (CNIL), Case 507/17 Sept. 24, 2019, http://curia.europa.eu/juris/document/document.jsf?text=&docid=218105&pageIndex=0&doclang=EN&mode=req&dir=&occ=first&part=1&cid=915058 [https://perma.cc/4Z4B-8W2D]; Jennifer Daskal, *Internet Censorship Could Happen More than One Way,* the Atlantic (Sep. 25, 2019), https://www.theatlantic.com/ideas/archive/2019/09/europe-gives-internet-speech-reprieve/598750/ [https://perma.cc/G2BS-TNG7] The case has spawned an active debate and commentary. Compare Nani Jansen Reventlow et al., "A French Court Case Against Google Could Threaten Global Speech Rights," *Washington 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/6AYZ-JX7R]. Reventlow supported Google in avoiding "a precedent that others will inevitably use to censor search results they don't like." Also, Frank Pasquale, "Reforming the Law of Reputation," *Loyola University Chicago Law Journal* 47 (2015): 515, 517. Pasquale stated, "Such removals 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," *New York Times*, Aug. 5, 2015, https://www.nytimes.com/2015/08/06/

different case, the ECJ gave the green light to Austria's efforts to mandate global takedowns and keep-off orders on a global scale to decide whether allegedly infringing material has to be removed globally or whether the de-indexing can be limited to searches emanating from the European Union.[44]

This is not the first time in which France and the United States have clashed over speech rights. The Yahoo! case over the sale of Nazi memorabilia—permitted in the United States but prohibited in France—is a precursor of the dispute regarding the right to be forgotten. Although Yahoo! initially claimed that it could not technically block just French residents' access to the relevant auction site, independent technical experts revealed that in fact it could do so with about 90 percent accuracy, and it was ordered to do so.[45] 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 the CNIL has deemed this insufficient, asserting that individual rights will be insufficiently protected if accessible at all.

A similar dispute also played out with respect to the linking of material that violates Canada's intellectual property laws. In that case, a Canadian court found that a company named Datalink had stolen trade secrets from a company named Equustek and was selling, over the internet, a competing counterfeit product. Datalink fled the jurisdiction and continued to operate from an unknown location. When Equustek requested that Google remove all links to Datalink, it did so—but only for searches stemming from its default Canadian domain, google.ca. It left the links available to those searching from google.com or from outside Canada. Equustek brought an action against Google, seeking a global takedown of all the links.

Google argued that Canadian courts did not have jurisdiction to issue an injunction with such broad extraterritorial effect, that doing so would set a dangerous precedent, and that it would interfere with the freedom of expression. The Canadian Supreme Court disagreed. As the Court put it, "The problem in this case is occurring online and globally. The Internet has no borders—its natural habitat is global. The only way to ensure that the interlocutory injunction attained its objective was to have it apply where Google operates—globally."[46] It also rejected the notion that this kind of injunction

technology/personaltech/right-to-be-forgotten-online-is-poised-to-spread.html?_r=1 [https://perma.cc/BZX9-HSW4].

[44] Jennifer Daskal, *A European Court Decision May Usher in Global Censorship*, Slate (Oct. 3, 2019), https://slate.com/technology/2019/10/european-court-justice-glawischnig-piesczek-facebook-censorship.html [https://perma.cc/7636-DER2]

[45] See La Ligue Contre le Racisme et L'Antisésmistisme et L'Union des Étudiants Juifs de France c. Yahoo! Inc. et Société Yahoo! France Interim Court Order, Tribunal de grande instance 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.

[46] Equustek case, Canadian Sup. Court (June 28, 2017) Par. 41, https://scc-csc.lexum.com/scc-csc/scc-csc/en/item/16701/index.do [https://perma.cc/E34A-PT4E].

would in any way interfere with the freedom of expression, given the underlying conduct at issue.

In response, Google filed for an injunction in a U.S. court, seeking to prevent enforcement. In a November 2017 ruling, the U.S. district court granted a preliminary injunction in favor of Google.[47] The court concluded that Google, as an intermediary provider, is protected by the Communications Decency Act from liability for infringing content produced by Datalink. It further concluded that, by forcing intermediaries to remove links to third-party material, the Canadian Supreme Court ruling "threatens free speech on the global Internet."[48] Of note, Equustek, the Canadian company that sought the takedown, did not appear in the case. U.S. court order in hand, Google asked the Canadian court to revise its initial ruling, but the Canadian court refused.[49]

These and other related cases raise important, and still highly contested, questions about whose rules govern and who gets to decide.[50] German law, for provides for the fining of social media companies—up to 50 million euros—if they fail to take down content that violates their hate speech laws.[51] It is not yet clear whether the data must be taken down globally or whether the law could be dealt with via geographic filtering. Other countries, including Turkey, have since pointed to Germany's law to support broad-based content regulations as well.

One possible, but particularly unsatisfactory answer, is that offered by China—for states to increasingly build closed-off internets with great firewalls. This would allow states to regulate content locally. But it also has huge costs to the free flow of information, to the economic growth potential of the internet, and global innovation. The prospect of harmonization across borders will conversely require states to tackle hard questions about the norms that apply and who gets to decide—with the possibility of and arguable need for different answers depending on the kind of speech being regulated.

35.1.3 Privacy Regulations and Efforts to Reassert Territorial-Based Controls

The European Union's far-reaching GDPR took effect in May 2018. In addition to the right to be forgotten, the GDPR mandates a number of additional privacy and data pro-

[47] Google v. Equustek, 2017 WL 5000834 (N.D. Ca. Nov. 2, 2017). [48] Ibid., *5.

[49] See Equustek Sols. Inc. v. Jack (*Equustek 2018*), 2018 BCSC 610, 19–21 (Can.); Keith Frasier, "Google Seeks to Lift B.C. Court Injunction Blocking Access to Websites," *Vancouver Sun*, Mar. 6, 2018, http://vancouversun.com/news/local-news/google-seeks-to-lift-b-c-court-injunction-blocking-access-to-websites [https://perma.cc/35AY-WE3Z].

[50] For a further discussion, see Jennifer Daskal, *Speech Across Borders*, 105 Va. L. Rev. 1605 (2019), https://www.virginialawreview.org/volumes/content/speech-across-borders.

[51] See, e.g., Soraya Sarhaddi Nelson, "With Huge Fines German Law Pushes Social Networks to Delete Abusive Posts," *NPR Morning Edition*, Oct. 31, 2017, https://www.npr.org/sections/parallels/2017/10/31/561024666/with-huge-fines-german-law-pushes-social-networks-to-delete-abusive-posts [https://perma.cc/CUR7-FD7V].

tection measures. Among other things, it increases the number of disclosures that must be made before an entity can process personal data;[52] lays out specific limitations on the cross-border transfer of data; imposes relatively strict "consent" requirements for the certain processing of personal data;[53] restricts the scope of permissible "profiling";[54] obliges a range of companies to impose data protection officers;[55] and includes new breach notification requirements.

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 EU subjects, or "the monitoring of [the] behavior" of EU-based subjects.[56] The GDPR thus represents 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. Just about any company that wants to serve customers in the European Union needs to comply with these requirements or be subject to potentially large fines.[57] And in fact, informal conversations suggest that companies doing business in the European Union implementing at least some key requirements globally rather than seeking to segregate their responses by geography.

Of particular note, the GDPR also includes fairly stringent restrictions on the transfer of EU resident data outside the European Union—building on transfer restrictions included in preexisting data protection directives. Transfers of personally identifying information are permitted in certain, limited conditions only. Absent explicit consent by the data subject explicitly, such transfers are only permitted if there are "adequate" privacy protections in place. This can be done either based on a country-level adequacy

[52] GDPR, art. 15. [53] Ibid., arts. 7, 9. [54] Ibid., arts. 22, 24, 60, 63, 71, 73.

[55] Ibid., art. 37. 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." See also ibid., art. 39, which lays 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," *The Privacy Advisor* (blog), *International Association of Privacy Professionals*, Jan. 7, 2016, https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-2-the-mandatory-dpo/[https://perma.cc/226S-5Z84].

[56] GDPR, art. 3(2).

[57] This is part of a broader trend. See, e.g., Dan Jerker B. Svantesson, "The (Uncertain) Future of Online Data Privacy," *Masaryk University Journal of Law & Technology* 9 (2015): 129, 131. Svantesson states, "[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."

determination, specific bilateral agreements that specify the conditions that companies must meet to justify transfers, or company-level agreements.

The treatment and reaction of the United States is instructive. The United States has never received a country-level adequacy determination. But it had, until 2015, an agreement in place known as the Safe Harbor Framework, pursuant to which companies could self-certify that they met certain requirements so as to allow the transfer of personal data from the European Union to the United States. In 2015, however, the ECJ struck down the Safe Harbor Framework, largely due to concerns about U.S. intelligence surveillance in the wake of the Snowden revelations.[58] Some 4,700 companies had relied on the Safe Harbor Agreement at the time.[59]

Since then, the European Union and the United States have negotiated the replacement Privacy Shield Framework, which is currently relied on by thousands of companies as a basis for engaging in the cross-continental transfer of personal data.[60] The agreement was conditioned on a series of changes in U.S. law and policy, all designed as increasing privacy protections.[61] A range of companies also rely on what are known as standard contractual clauses as a basis for transferring data to the United States as well.[62]

Both Privacy Shield and standard contractual clauses are now subject to legal challenge as well—based on ongoing concerns about the adequacy of privacy protections in U.S. law, the reach of U.S. surveillance, and the opportunities (or lack thereof) for accountability.[63] In October 2017, the Irish High Court concluded that there are "well

[58] *See* Case C-362/14, Maximillian Schrems v. Data Prot. Comm'r, 2015 E.C.R., ¶¶ 94–95, http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=EN [https://perma.cc/3H52-6LS8].

[59] Natasha Lomas, Europe's Top Court Strikes Down Safe Harbor Data Transfer Agreement With U.S., Tech Crunch, (Oct. 6, 2015), https://techcrunch.com/2015/10/06/europes-top-court-strikes-down-safe-harbor-data-transfer-agreement-with-u-s/ [https://perma.cc/9HHB-LHNZ].

[60] See Sam Schechner, "Europe's Top Court to Review Privacy," *Wall Street Journal*, Oct. 4, 2017.

[61] Specific reforms cited as important to the European Union include: the adoption of the Judicial Redress Act, which extends protections of the Privacy Act of 1974 to the citizens of the European Union and other designated foreign countries (see Judicial Redress Act of 2015, Pub. Law No. 114-126 (2016)); the passage of USA Freedom Act, which, among other things, put an end to the government's bulk collection of domestic telephony metadata (see USA FREEDOM Act of 2015, Pub. Law No. 114-23 (2015)); and adoption of new executive branch guidance designed to better protect the privacy interests of foreigners (see Section 4 of The White House: President Barack Obama, "Presidential Policy Directive—Signals Intelligence Activities," Jan. 17, 2014, https://obamawhitehouse.archives.gov/the-press-office/2014/01/17/presidential-policy-directive-signals-intelligence-activities [https://perma.cc/HMH5-PCBL]).

[62] Other possible mechanisms for supporting the cross-continental transfer of personal data include consent by the data subject (although the standard for finding valid consent can be hard to meet); binding corporate rules (although these only permit intracorporation transfers and do not allow transfers to unaffiliated entities, such as customers and suppliers); and reliance on approved codes or conduct. See Lothar Determan, Brian Hengesbaugh, and Michaela Weigl, "The E.U.-U.S Privacy Shield Versus Other EU Data Transfer Compliance Options," *Bloomberg BNA*, Sept. 12, 2016. The article details various transfer options.

[63] See Case T-670/16, Dig. Rights Ireland v. Comm'n, 2016 O.J. (C 410) 26; Data Prot. Comm'r v. Facebook Ireland Ltd. & Maximillian Schrems (Schrems II), [2017] 2016 No. 4809 P (H. Ct) (Ir.) (Oct. 3, 2017), https://iapp.org/media/pdf/resource_center/IrishHC-Fb-Schrems-decision-10-17.pdf [https://perma.cc/7HNQ-9KXS]. The Court referred the case to the ECJ.

founded concerns" about the adequacy of the privacy protections provided for by standard contractual clauses. The Court's ruling focused on the reach of U.S. foreign intelligence surveillance and the perceived absence of effective remedies.[64] The case is now pending before the ECJ.[65] And depending on how the ECJ rules, both Privacy Shield and the standard contractual clauses could be in jeopardy.

This is an example of the European Union using its market power to compel privacy-protective changes in other countries as well. With respect to the data transfer cases, the demands are countrywide—demanding broad changes in U.S. surveillance laws and privacy policies. Other regulations require privacy-protective policies within the companies themselves—policies that then are, at least in some cases, exported to the jurisdictions where they operate.[66]

Meanwhile, other attempts to assert territorial-based controls have reified the sovereignty-territoriality link, imposing a range of data localization mandates as a means of reasserting local control. Unlike the EU measures that seek to effectively raise privacy protections via privacy-linked limitations on transfers, such mandates seek to control access to data by demanding that data be held locally, regardless of conditions elsewhere. And they are proliferating.[67]

35.2 Implications

The rise of data and multinational companies that control our data is challenging notions of sovereignty, in particular the pervasive assumption of unilateral and exclusive control over people and things in one's territory. But this is not the same as death of sovereignty or even territorial-based sovereignty. To the contrary, states have found ways to assert territorial-based controls over data as well the people and companies that manage our data. But they increasingly do so via the multinational corporations that manage our data, thus setting—or at least seeking to set—global policy, but via local regulation. Meanwhile, the private parties that manage so much of the world's data are themselves increasingly setting the rules.

This both creates conflict and holds out the promise for new kinds of harmonization. Often, this harmonization may be invisible—via decisions of private actors in deciding to acquiesce to the demands of a particular state. Or in making independent policy determinations that are applied globally. In other instances, harmonization will require the coming together of states to mediate conflicting claims. At least initially, this is much more likely to happen on a bilateral or multilateral basis, rather than the development of

[64] Schrems II, 2016 No. 4809 P at ¶ 334. [65] Ibid.

[66] For a broader discussion of these and related efforts by the EU to set global rules, see Anu Bradford, The Brussels Effect: How the European Union Rules the World (Oxford University Press 2020).

[67] See, e.g., Anupam Chander and Uyen P. Le, "Data Nationalism," *Emory Law Journal* 64 (2015): 677.

universal norms. Bilateral agreements pursuant to the CLOUD Act provides one such example. But it is a form of access that will, at least pursuant to current legislative initiatives, only be extended to like-minded countries, based on a determination that the partner countries have in place sufficient baseline protections for privacy and speech rights and are committed to fair process and the rule of law. Countries that don't meet these requirements may be left out, further exacerbating the conflict between those that are "in" and those that are "out."

Resolution of these issues is a critically important and complex project, well beyond the scope of this chapter. My goal here is simply to highlight the changing sources of power and control. That, after all, is the first step toward either harmonization or peaceful coexistence, coupled with meaningful procedural and substantive safeguards of core rights and liberties that is, in my view, the ultimate goal. There is a cross-cutting need to consider new forms of accountability to deal with the shift in power to private actors and the changing ways in which both national and international rules adopted in response. Specifically, I suggest two.

First, increased transparency and notice requirements imposed on the companies that manage so much of the world's data. Some such reporting on things like aggregate numbers of law enforcement requests and takedown is already done voluntarily by some of the larger tech companies, but more could and should be mandated. It should not be left to the discretion of the companies, each of which provide the information in their own and often hard-to-compare format. Moreover, while most of the major U.S.-based companies now provide this kind of transparency on their own accord, there is no guarantee new entrants will do so in the future and no accountability if they fail to or insufficiently do so going forward.

Second, increased oversight and review. As governments increasingly access data outside their borders without relying on the MLA process, an important governmental check on access is elminated. In its place, governments should put in place effective oversight mechanisms to ensure the requesting government's substantive and procedural requirements are being met. Governments also should also provide a mechanism for companies to raise questions and concerns about requests that appear to fall short of the required protections. Similarly, external reviewers should oversee and provide public accountings of the ways companies are implementing the right to be forgotten, restrictions on hate speech, and their own terms of services and other contractual obligations. This would at least have the effect of providing an initial check, increased accountability and transparency, and set of guiding rules to govern the private sector decision-making.

These are modest but important recommendations—stemming from a recognition that private governments are no longer the primary, or even most important, enforcers of security, privacy, and speech rights. A range of private decisions made by major multinational companies have implications across multiple borders and for individuals across the globe. Broader more systematic reforms are additionally needed to align private company incentives with the chosen normative goals. And there is a need for new, robust forms of accountability, separate and apart from the voting booth, to reflect the new reality.

35.3 Conclusion

Data and the governments that manage our data are both unterritorial and multiterritorial. Yet, they operate in a world of territorial-based states. The reality is messy and complicated, yielding a shift in power, and resulting in multiple actors seeking to control or access the same data simultaneously. But whereas some of the messiness can be accommodated, some requires new, concerted efforts at harmonization and new norm development so as to better respect the sovereign interests of state, reduce the incentives in favor of Balkanization of the internet that tend to facilitate the undercutting of rights, and set baseline protections designed to enhance privacy and protect against abuse in the process. Meanwhile, new tools are needed to hold the key players to account.