HUMAN RIGHTS

Law Enforcement Access to Data Across Borders: The Evolving Security and Rights Issues

Jennifer Daskal*

INTRODUCTION

A revolution is underway with respect to law enforcement access to data across borders. Frustrated by delays in accessing data located across territorial borders, several nations are taking action, often unilaterally, and often in concerning ways. Several nations are considering (or have passed) mandatory data localization requirements, pursuant to which companies doing business in their jurisdiction are required to store certain data, or copies of such data, locally. Such measures facilitate domestic surveillance, increase the cost of doing business, and undercut the growth potential of the Internet by restricting the otherwise free and most efficient movement of data. Meanwhile, a range of nations – including the United Kingdom, Brazil, and others – are asserting that they can unilaterally compel Internet Service Providers (ISPs) that operate in their jurisdiction to produce the emails and other private communications that are stored in other nation's jurisdictions, without regard to the location or nationality of the target. ISPs are increasingly caught in the middle – being forced to choose between the laws of a nation that seeks production of data and the laws of another nation that prohibits such production. In 2015, for example, Brazilian authorities detained a Microsoft employee for failing to turn over data sought by Brazil; U.S. law prohibited Microsoft from complying with the data request.[1] Governments also are increasingly incentivized to seek other means of accessing otherwise inaccessible data via, for example, use of malware or other surreptitious forms of surveillance.

The problems associated with law enforcement access to data across borders are just beginning to get the attention they deserve – overshadowed in large part by the heavy focus on intelligence collection, particularly in the aftermath of the Edward Snowden revelations. But a number of governments, corporations, and members of civil society are now focused on the issue as one of increasing importance. In February 2015, the United States House Judiciary Committee

---

* Jennifer Daskal is an assistant professor at American University Washington College of Law. Special thanks to NATO Cooperative Cyber Defence Center of Excellence for encouraging and supporting this article, to the Cross-Border Data Request (CBDR) Working Group for the many helpful conversations and to Andrew K. Woods for his comments on an earlier draft of this article. © 2016, Jennifer Daskal.

1. Brad Smith, *In the Cloud We Trust*, MICROSOFT STORIES, http://news.microsoft.com/stories/inthecloudwetrust.

held a hearing on law enforcement access to data across borders and conflicts of laws.[2] The U.K. Home Office has described the creation of streamlined processes for obtaining data held by U.S.-based providers as one of their most important priorities;[3] the issue is high on the agenda of a number of other foreign governments as well.[4] A handful of scholars also are now exploring the complicated jurisdictional, privacy, and security questions that have arisen.[5] This article seeks to add to this nascent, yet growing literature. Its aims are three-fold: to provide the key background, to highlight the need for action, and to suggest a way forward.

A caveat up front: the article is U.S.-centric, and is so for a reason. While the problem of cross-border access to data is inherently international, the United States has an outsized role to play, given a combination of the U.S.-based provider dominance of the market, blocking provisions in U.S. law that prohibit the production of the content of electronic communications (such as emails) to foreign-based law enforcement, and the particular ways that companies are interpreting and applying their legal obligations. The approach taken by the United States is likely to become a model for others, thus providing the United States a unique opportunity to set the standards – standards that ideally will protect privacy, security, and the growth of an open and global Internet. The

---

2. *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests*: *Hearing Before the H. Comm. on the Judiciary*, 114th Cong. (2016) [hereinafter *Judiciary Comm. Hearing*].

3. Meeting, UK Embassy Staff, May 9, 2016.

4. *See, e.g.,* Council of Europe Cyber Crime Committee (T-CY), *Transborder Access to Data and Jurisdiction: Options for Further Action by the T-CY*, Report prepared by the Ad-hoc Subgroup on Transborder Access and Jurisdiction, adopted by the 12th Plenary of the T-CY (Dec. 3, 2014), http://www.coe.int/t/dghl/cooperation/economiccrime/Source/Cybercrime/TCY/2014/T-CY(2014)16_TBGroupReport_v17adopted.pdf; Council of Europe Cybercrime Convention Committee (T-CY), *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 (16 Sept. 2016), https://rm.coe.int/CoERMPublicCommonSearchServices/DisplayDCTMContent?documentId=09000016806a495e.

5. *See, e.g.*, Andrew Keane Woods, *Against Data Exceptionalism*, 68 STAN. L. REV. 729 (2016); Zachary Clopton, *Territoriality, Technology, and National Security*, 83 U. CHI. L. REV. 45 (2016); Vivek Krishnamurthy, *Cloudy with a Conflict of Laws*, BERKMAN CTR. FOR INTERNET & SOC'Y AT HARVARD LAW SCH., Research Pub. No. 2016-3 (Feb. 16, 2016); Peter Swire & Justin Hemmings, *Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program*, GEORGIA TECH SCHELLER COLL. OF BUS. Research Paper 38 (2016); Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L. J. 326 (2015). *See also* Jennifer Daskal, *A New UK-US Data Sharing Agreement: A Tremendous Opportunity, If Done Right*, JUST SECURITY (Feb. 8, 2016), https://www.justsecurity.org/29203/british-searches-america-tremendous-opportunity; Jennifer Daskal & Andrew K. Woods, *Cross-Border Data Requests: A Proposed Framework,* JUST SECURITY (Nov. 24, 2015), https://www.justsecurity.org/27857/cross-border-data-requests-proposed-framework; Michael Chertoff & Paul Rosenzweig, *A Primer on Globally Harmonizing Internet Jurisdiction and Regulation*, GLOBAL COMM'N ON INTERNET GOV. No. 10 (Mar. 2015), https://www.cigionline.org/sites/default/files/gcig_paper_no10_0.pdf; Jonah Force Hill, *Problematic Alternatives: MLAT Reform for the Digital Age*, HARV. NAT'L. SEC. J. ONLINE (Jan. 28, 2015), http://harvardnsj.org/2015/01/problematic-alternatives-mlat-reform-for-the-digital-age; Albert Gidari, *MLAT Reform and the 80 Percent Solution*, JUST SECURITY (Feb. 11, 2016), https://www.justsecurity.org/29268/mlat-reform-80-percent-solution; David Kris, *Preliminary Thoughts on Cross Border Data Requests*, LAWFARE (Sept. 28, 2015), http://www.lawfareblog.com/preliminary-thoughts-cross-border-data-requests.

alternative is a Balkanized Internet and a race to the bottom, with every nation unilaterally seeking to access sought-after data, companies increasingly caught between conflicting laws, and privacy rights minimally protected, if at all.

I. BACKGROUND: DATA ACROSS BORDERS

Data no longer respects international boundaries. When Jack in San Francisco, California sends an email to Jill in New York, it may take a direct route from California to New York, or it may travel through Canada, or even the United Kingdom, before arriving at its intended destination. When one stores data in the cloud, that data may either be held locally or in storage centers dispersed as far as India, Ireland, and Chile. If the database is large enough, it may even be partitioned into multiple parts – some of which may be stored territorially and some extraterritorially.[6]

Law enforcement officials around the world are, as a result, increasingly seeking the production of data held outside their borders, even in the investigation of local crime. And they are chafing at territorial-based restrictions on access. Imagine, for example, an investigative officer in London trying to solve a local murder. He suspects it is an affair gone bad. But he soon learns that the email accounts of the victim, the victim's lover, and the victim's spouse are all controlled by Google or Microsoft and located on a server in California. If the provider were U.K.-based, he could, assuming compliance with appropriate U.K. processes, directly compel the production of the emails. And he would likely get access to the data within days, if not sooner. But when he sends the request to Google or Microsoft, he gets something akin to the following response: "Sorry, we are prohibited under U.S. law from turning over the content of communications without a warrant issued by a U.S. judge or magistrate based on probable cause. Go talk to our Department of Justice."

He does, initiating a diplomatic request for the data, employing the procedures spelled out in the Mutual Legal Assistance Treaty between the United States and United Kingdom. The officer quickly learns that the average time to process such a request is ten months.[7] First, the Department of Justice reviews the request. Once approved, it is forwarded to the relevant U.S. Attorney's Office. Second, a federal prosecutor obtains a warrant from a U.S.-based magistrate based on a U.S.-based standard of probable cause in order to compel production of the sought-after data. Needless to say, processing these foreign requests for data is not often at the top of most U.S. Attorneys' priority lists. Third, the warrant is served on the relevant Internet Service Provider (ISP).

---

6. *See* Daskal, *The Un-Territoriality of Data*, *supra* note 5, at 365-378; Frederick T. Davis, *A U.S. Prosecutor's Access to Data Stored Abroad – Are There Limits?*, 49 THE INT'L LAWYER 1, 8-10 (2015).

7. *See, e.g.*, 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 226-29 (2013) (noting that the United States takes an average of ten months to respond to official requests made through the MLAT process for email records).

Fourth, the data, once produced, is routed back to the Department of Justice, where it is again reviewed before finally being transferred to the requesting government.[8] Meanwhile, the murder goes unsolved.

Some of these delays can be minimized by improvements to the mutual legal assistance (MLA) system, including the creation of on-line request processes, the designation of a single point of contact within the U.S. Attorneys' offices for processing such requests, and increased funding for the division in the Department of Justice that handles such requests.[9] That said, even with increased resources and streamlining, the multi-step MLA process – which will still require that a U.S. prosecutor obtain a U.S. warrant in order to access the data – is likely to be time-consuming. Or at least more time-consuming than would be the case if foreign governments could directly access the data from U.S.-based providers. Foreign governments would still be required to get a U.S. warrant based on a U.S. standard of probable cause even when the United States' only connection to the data is that it happens to be controlled by a U.S.-based provider or located on U.S. soil.

Moreover, if the U.K. government wanted to engage in the interception of real-time communications – such as a Google chat between two U.K. residents – it would simply be out of luck, no matter how many improvements are made to the current MLA system. The MLA system does not provide a mechanism for foreign governments to access real-time communications transmitted across U.S. soil, even if the target of the surveillance is a foreigner located outside the United States. The only way the U.K. would be able to get the data would be if it could convince the United States to open what is known as a "joint investigation," and then the cooperating U.S. agents could seek a wiretap order under U.S. domestic authorities.

Foreign governments are frustrated, and they are responding in a number of troubling ways – all designed to facilitate direct access to sought-after data. The range of responses include:

- *Mandatory data localization requirements*, pursuant to which the content of communications (or a copy of such content) involving a country's residents and/or citizens are required to be held in-country.[10] This enables domestic law enforcement to access the data pursuant to domestic legal

8. *See* Peter Swire & Justin Hemmings, *Stakeholders in Reform of the Global System for Mutual Legal Assistance*, GEORGIA TECH SCHELLER COLL. OF BUS., Research Paper No. 32 2-5 (2015) (describing delays caused by the MLA system and the reactions of foreign governments).

9. *See* CLARKE ET AL., *supra* note 7, at 226-229; *see also* U.S. DEP'T OF JUSTICE, FY 2017 BUDGET REQUEST, NATIONAL SECURITY 4-5 (emphasizing the need to hire additional personnel to assist with mutual legal assistance matters; request was granted in part and additional hiring has ensued).

10. *See, e.g.*, Sergei Blagov, *Russia's 2016 Data Localization Audit Plan Released*, BLOOMBERG LAW, Jan. 13, 2016, http://www.bna.com/russias-2016-data-n57982066291; Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 EMORY L.J. 677 (2015) (surveying localization laws); Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information* (Sept. 2015) (documenting data localization trends); JONAH FORCE HILL, THE GROWTH OF DATA LOCALIZATION

process, without having to make a diplomatic request to the United States. But such requirements increase the costs to ISPs and other businesses that manage users' data by forcing them to build additional data storage centers and maintain copies of data in-country even when doing so is inefficient; this, in turn, undercuts the innovative potential of the Internet.[11] Data localization also facilitates domestic surveillance – ensuring that the local government can access sought-after data based on its own laws and processes, without having to rely on the MLA process, and without U.S. law having anything to say about the standards that apply.

- *Unilateral assertions of extraterritorial jurisdiction.* Current U.K. law, for example, as well as draft legislation designed to replace the expiring provisions in the current law, includes the authority to compel the production of stored content from any company that does business in its jurisdiction.[12] This authority to compel applies without limit based on the location of the data, the location of the provider's place of business, the target's nationality, or the target's place of residence.[13] Brazil has passed similar legislation as well,[14] and U.S. authorities have claimed an analogous authority in litigation with Microsoft.[15] Such unilateral assertions of

---

POST-SNOWDEN: ANALYSIS AND RECOMMENDATIONS FOR U.S. POLICYMAKERS AND BUSINESS LEADERS (2014) (describing the rise of data localization movements and analyzing the key motivating factors).

11. *See also* Swire & Hemmings, *supra* note 8, at 8-10 (describing costs to businesses, security, and human rights that result from localization laws).

12. *See* Data Retention and Investigatory Powers Act (DRIPA), 2014, c.27, § 4 (UK) (expires December 31, 2016); Investigatory Powers Bill, 2015-16, H.C. Bill [143] §§ 34(4), 35, 36(3) (UK) (specifying extraterritorial reach of authority to compel the production of the content of communications). U.K. officials suggested that a key goal of the DRIPA was to permit access to otherwise hard-to-obtain data in the control of U.S.-based providers. *See* INTELLIGENCE AND SEC. COMM. OF PARLIAMENT, REPORT ON THE INTELLIGENCE RELATING TO THE MURDER OF FUSILIER LEE RIGBY, 2014-15, H.C. 795, ¶¶ 457-460 (UK).

13. While the legislation specifies that "regard is to be had" to a possible conflict of laws, the legislation does not say whether and in what situations the laws of the nation in which the data is located would trump. DRIPA § 4(4). *See also* Data Retention and Investigatory Powers Bill, Explanatory Notes, 2014, H.L. 37, ¶¶ 16-17 (UK).

14. *See* Marco Civil (Law 12965/2014), art. 11, par. 2 (stating that Brazilian law governs Internet Service Providers operating abroad so long as they provide services to the Brazilian public).

15. *See* Brief for Appellee, *In re Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp.* (2d Cir. Mar. 9, 2015) (No. 14-2985-CV). Although the United States ultimately lost the case, *see* In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No.14-2985 (2d Cir. July 14, 2016), the Department of Justice has indicated that it will seek a statutory change to permit broad authority to compel, without regard to the location of data. The U.S. government plans to seek legislation to explicitly grant law enforcement officials the authority to compel the production of data that is located extraterritorially. *See* Letter from Peter J. Kadzik, Assistant Attorney Gen., to Joseph R. Biden, President, U.S. Senate at 2-3 (July 15, 2016), http://www.netcaucus.org/wp-content/uploads/2016-7-15-US-UK-Legislative-Proposal-to-Hill.pdf (warning that "[i]f this decision stands, or is extended to other parts of the country, the U.S. would not have, under 2703, access to data necessary to advance important U.S. investigations that protect the safety of Americans and could not obtain reciprocal benefits from other countries. The Administration intends to promptly submit legislation to Congress to address the significant public safety implications of the *Microsoft* decision.").

extraterritorial jurisdiction put companies in the crosshairs between conflicting laws, with one country compelling production of data and another country prohibiting it.[16] Such laws also facilitate domestic surveillance by authorizing law enforcement to compel production of data wherever located, based on the requesting country's own laws.

- *Threats against employees or officers of local subsidiaries* for failing to turn over sought-after data, even in situations when another country's laws prohibit them from doing so. In January 2015, for example, a Microsoft executive was arrested and criminally charged for his failure to produce data requested by Brazilian authorities; U.S. law – namely the Stored Communications Act – barred him from doing so.[17]

- *Mandatory anti-encryption regimes* (e.g., mandatory backdoors) that facilitate live interception of the data as it transits through the requesting government's jurisdiction and thereby provide an alternative way to access sought-after communications.[18] This undermines the security of the Internet – introducing vulnerabilities into the system that can be exploited not just by law enforcement, but by cyber-criminals as well.

- *Increased use of malware* and other opaque and less accountable means of accessing the data that, like anti-encryption measures, weaken the security for all users.[19]

Such responses by foreign governments threaten privacy, undermine security, harm business interests, and diminish the productive potential of the Internet over time. A growing chorus of voices is, as a result, warning of the consequences of the current state of affairs and urging change.[20]

When it comes to non-content information, the situation is very different. Whereas U.S. law generally prohibits U.S.-based providers from turning over the *content* of communications directly to foreign law enforcement, no such

16. *See* John Ribeiro, *Microsoft says tech companies 'whipsawed' by conflicting laws on global data transfer,* IDG NEWS SERV. (Feb. 23, 2016), http://www.pcworld.com/article/3036977/tech-events-dupe/microsoft-says-tech-companies-whipsawed-by-conflicting-laws-on-global-data-transfer.html.

17. *See* Brad Smith, *supra,* note 1.

18. *See* Swire & Hemmings, *supra* note 8, at 5-6 (describing foreign governments' incentives to mandate access to encrypted communications transiting through their jurisdiction); *cf.* Regulation of Investigatory Powers Act 2000, c. 23 §§ 49-51 (UK) (laying out situations in which the U.K. government can mandate providers to assist with de-encryption).

19. *See* Ahmed Ghappour, *Justice Department Proposal Would Massively Expand FBI Extraterritorial Surveillance*, JUST SECURITY (Sept. 16, 2014), https://www.justsecurity.org/15018/justice-department-proposal-massive-expand-fbi-extraterritorial-surveillance (explaining how malware could be used to subvert otherwise applicable territorial limits on direct access to sought-after data).

20. *See, e.g.*, *International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests*: *Hearing Before the H. Comm. on the Judiciary*, *supra* note 2 (statements of Brad Smith, President and Chief Legal Officer, Microsoft Corp.; Michael Chertoff, Exec. Chairman and Co-Founder, The Chertoff Group; David Kris, Executive Vice President and General Counsel, Intellectual Ventures); *see also* articles cited *supra* note 5.

prohibitions apply with respect to *non-content* data.[21] Already, U.S.-based companies are, according to their own transparency reporting, responding to tens of thousands of foreign government requests for non-content data each year – data that ranges from things like subscriber names and addresses, IP addresses, and credit card information.[22] Notably, there are no procedural requirements or substantive standards governing when and under what circumstances companies can respond to such requests from foreign governments. This is true even when foreign governments are seeking the non-content data of U.S. citizens or legal permanent residents, or of other persons physically located within the United States. Informal conversations suggest that the major U.S. providers subject such foreign-based requests to a robust vetting process, yet such vetting is voluntary and companies apply varied standards in responding to such requests.

By comparison, U.S. government officials must obtain either a subpoena or court order (depending on the kind of data sought) in order to obtain the same non-content data that companies can provide to foreign governments voluntarily. Court orders, which are required for the kinds of non-content data that can reveal information about a target's associations and activities, demand a predicate finding of "specific and articulable facts showing that there are reasonable grounds to believe that the records or information sought are relevant and material to an ongoing criminal investigation."[23] U.S. law enforcement officials are, as a result, held to a higher standard under U.S. law than foreign governments when they are seeking the exact same non-content data from the exact same providers.

II. THE KEY ISSUES

As the foregoing illustrates, the issues surrounding law enforcement access to data across borders raise normative and pragmatic questions about territoriality, sovereignty, and enforcement jurisdiction. Whose rules govern? Does enforcement jurisdiction turn on the location of the data or something else? When, and in what situations, is a state entitled to unilaterally seize data located in another state's territory? The answers to these questions have important implications for security, privacy, and the growth of the Internet. They also are of growing importance to the multi-national corporations that increasingly find themselves

21. 18 U.S.C. § 2702(a)(3) (2006) prohibits the disclosure of non-content data to "any governmental entity." But, "governmental entity" is defined as "department or agency of the *United States* or any State or political subdivision thereof."18 U.S.C. § 2711(4) (2009) (emphasis added). There is no analogous prohibition on the disclosure of non-content data to foreign government officials.

22. *See, e.g.*, APPLE, REPORT ON GOVERNMENT INFORMATION REQUESTS (July 1 – Dec. 31, 2015), http://www.apple.com/legal/privacy/transparency/requests-20141231-en.pdf; FACEBOOK, GOVERNMENT REQUESTS REPORT (Jan. 2013 – Dec. 2015), https://govtrequests.facebook.com; GOOGLE, TRANSPARENCY REPORT: REQUESTS FOR USER INFORMATION (Dec. 2009 – June 2015), http://www.google.com/transparencyreport/userdatarequests; MICROSOFT, LAW ENFORCEMENT REQUESTS REPORT (Jan. 2013 – Dec. 2015), https://www.microsoft.com/about/corporatecitizenship/en-us/reporting/transparency.

23. 18 U.S.C. § 2703(d) (2009).

caught in a difficult conflict of laws. The following very briefly outlines the security and economic interests at stake. It then turns to a more detailed examination of the privacy and jurisdictional issues that are being raised.

A. Security

The primary security concerns are self-evident. Law enforcement seeks access to data for the purposes of solving and preventing crime. The combination of blocking provisions that prevent foreign nations from directly accessing data relevant to a legitimate law enforcement investigation, and the laborious, time-consuming data-sharing arrangements impinges on the ability to fight and solve crime. This has obvious security costs. Moreover, the security costs are likely to grow over time, as more and more evidence becomes digitalized, even in run-of-the-mill local crimes.

But there is another, less obvious security cost as well. Governments are increasingly being incentivized to find alternative means to obtain access to otherwise inaccessible data. These include: anti-encryption measures that enable the government to access the data as it transits its jurisdiction; the use of malware as a means of accessing otherwise inaccessible data; and other surreptitious means of accessing sought-after data. Such measures come with their own security costs – potentially making the Internet less secure not just for the targets of the government surveillance, but for all users.[24]

B. Economic

The economic costs that result from the status quo also are readily apparent. Absent harmonization of key jurisdictional issues, providers are increasingly caught between conflicting laws in ways that make it difficult to operate internationally. They have to choose which of two competing legal obligations to comply with, and may face fines – or in some cases criminal prosecution – in one or both of the competing jurisdictions. At some point, the costs of doing international business will simply be too high for some providers (especially smaller-scale providers), and they will have to avoid or pull out of certain markets.

Data localization mandates – pursuant to which providers are required to store a copy of certain data in the requiring country's territorial jurisdiction – provide a potential way around the conflict of laws problem; they help ensure local jurisdiction over sought-after data. But they increase the cost of doing business internationally, making it harder for small businesses and start-ups to enter and stay in the market. Such measures also undercut the efficiency and economic gains that would otherwise result from the free flow of data across borders.

---

24. *See, e.g.*, Hal Abelson et al., *Keys Under Doormats: Mandating Insecurity by Requiring Government Access to All Data and Communications*, 1 J. CYBERSECURITY 69 (2015); CRYPTOGRAPHY'S ROLE IN SECURING THE INFORMATION SOCIETY (Kenneth Dam & Herbert Lin, eds., 1996).

C. Privacy and Related Human Rights

The rules and practices governing cross-border access to data squarely implicate the right to privacy – a right that is enshrined in the United Nations (U.N.) Declaration of Human Rights,[25] International Convention on Civil and Political Rights (ICCPR),[26] the European Charter on Human Rights,[27] the European Union Charter of Fundamental Rights,[28] and a range of other regional and international instruments. While the different instruments define privacy slightly differently, they share a common requirement that any interference with privacy be done in accordance with law, in pursuit of a legitimate aim, and in a manner that is proportionate to that aim.

In the United States, the right to privacy, at least vis-à-vis governmental collection of data, is protected by the Fourth Amendment, which prohibits unreasonable searches and seizures, and, in the context of the *content* of certain communications (such as emails) is widely understood to require a warrant based on probable cause.[29] This standard fully satisfies the human rights requirement that "no one shall be subject to arbitrary or unlawful interference with his privacy,"[30] and, as discussed below, is a standard that is higher than applied in most other countries as a precondition for governmental collection of data.

The cross-border collection of data also touches on the bucket of related rights that privacy protections safeguard, including the rights to free expression, freedom of conscience and religion, free assembly and free association, and health, among others. The potential concerns are two-fold. *First*, collection alone can put expressive, associational, and related rights at risk. Individuals may become fearful of fully exposing their opinions, religious beliefs, or associations due to the risk of monitoring. Individuals concerned about unwarranted access may also be less likely to communicate sensitive health information, thereby implicating the right to health.[31]

Second, collection can be, and often is, subsequently *used* to stifle such rights. As described in detail by the U.N. expert on the freedom of expression, states around the world engage in the censorship of legitimate critics,[32] impose

---

25. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, (Dec. 10, 1948).

26. International Covenant on Civil and Political Rights art. 17, Mar. 23, 1976, 999 U.N.T.S. 171 [hereinafter ICCPR].

27. European Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Nov. 4, 1950, 213 U.N.T.S. 222.

28. Charter of Fundamental Rights of the European Union arts. 7-8, Oct. 26, 2010, 2012 O.J. c 326, 391.

29. *See* United States v. Warshak, 631 F. 3d 266, 288 (6th Cir. 2010). *See also* Christopher Slobogin, *A Defense of Privacy as the Central Value Protected by the Fourth Amendment,* 48 TEX. TECH L. REV. 143-63 (2016).

30. ICCPR, *supra* note 26, art. 17(1).

31. Rep. of the Office of the United Nations High Comm'r for Human Rights, U.N. Human Rights Council, *Right to Privacy in the Digital Age*, ¶ 14, U.N. Doc. A/HRC/27/37 (June 30, 2014) [hereinafter REP. OF OHCHR].

32. *Id.* at ¶ 79.

a range of restrictions on the right to peaceful assembly, particularly in the run-up to elections,[33] and detain and prosecute journalists and bloggers for expressing "inconvenient" information.[34] Collected data also may be used to identify targets that are then subjected to arbitrary arrest or detention, or even worse, torture or other forms of cruel treatment. In some cases, collected data may even help direct the state to targets in kill operations – thereby potentially infringing on the right to life.[35]

In general, human rights law is better equipped to address the ways in which governments *use* data in abusive or illegitimate ways than as a tool for regulating *collection* itself.[36] After all, governments that stifle free expression, association, or democratic participation within its borders are engaging in overt violations of their human rights obligations – regardless of how or where the information used to target a particular individual was gathered. The use of human rights law as a tool for addressing harms that stem directly from the *collection*, by contrast, poses a series of tricky legal and policy questions – all at the heart of the issue of law enforcement access to data across borders.

1. The Key Considerations: Content of Communications

Any analysis of cross-border access to data must grapple with difficult questions about the baseline procedural and substantive requirements that apply to the collection of the sought-after data. The U.S. warrant requirement is unique to the United States and more robust than what is required in most other nations. Criminal law warrants must be signed off by a neutral magistrate or judge based on a probable cause finding that the data sought is evidence of a

33. Human Rights Council, Rep. of the Special Rapporteur on the Promotion and Prot. of the Right to Freedom of Op. and Expression, U.N. Doc. A/HRC/26/30, at ¶ 37 (May 30, 2014) [hereinafter REP. OF THE SPECIAL RAPPORTEUR].

34. *Id.* at ¶ 78-79; *see also* REPORTERS WITHOUT BORDERS, ROUND-UP OF JOURNALISTS KILLED WORLDWIDE 9 (Dec. 28, 2015), https://rsf.org/sites/default/files/rsf_2015-part_2-en.pdf (indicating that there are currently 153 journalists detained worldwide, and another 54 held hostage). Many others may be detained short-term or harassed in ways that are not covered by the reported statistics.

35. *See* REP. OF OHCHR ¶ 14, *supra* note 31:

> Other rights, such as the right to health, may also be affected by digital surveillance practices, for example where an individual refrains from seeking or communicating sensitive health-related information for fear that his or her anonymity may be compromised. There are credible indications to suggest that digital technologies have been used to gather information that has then led to torture and other ill-treatment. Reports also indicate that metadata derived from electronic surveillance have been analysed to identify the location of targets for lethal drone strikes. Such strikes continue to raise grave concerns over compliance with international human rights law and humanitarian law, and accountability for any violations thereof.

36. *See, e.g.*, U.N., Human Rights Council, Resolution, The promotion, protection, and enjoyment of human rights on the Internet, U.N. Doc. A/HRC/32/L.20 (adopted 1 July 2016) (emphasizing the right to freedom of expression on the Internet, condemning human rights abuses committed against persons for exercising their right to free expression on the Internet, and condemning the disruption of access to information online in a manner that violates international human rights).

crime.[37] Many nations authorize the collection of data based on authorizations signed by officials in the executive branch, without independent judicial review. In other cases, judicial review may be required, but the judiciary is independent in name only. Moreover, few nations employ a "probable cause" standard; many allow the collection of content based on a much lower standard of proof. And even when robust procedural and substantive standards are *generally* required, exceptions often apply in national security cases.[38] This means that, under current rules, foreign governments often struggle to meet the standards required to lawfully compel the production of content data held by a U.S. company in the United States. It is, in fact, one of the reasons that it takes so long for the United States to process foreign government requests for data. The office at the Department of Justice that handles such requests often has to send back initial requests, asking the requesting government to provide additional information in order to satisfy the United States' probable cause standard.

Interest in new cross-border agreements on expedited access to content data – such as that reportedly being discussed between the U.S. and U.K. governments[39] – stems in part from a desire to bypass what is perceived as the at-times onerous requirement of probable cause and time-consuming requirement of review by a neutral magistrate. Put another way, foreign governments want to be able to access sought-after data according to their own standards, which in many instances will be subject to fewer procedural and substantive protections than if the data were subject to the U.S. process.

This yields a series of important human rights considerations:

- In what situations, if ever, is it appropriate for requests for the content of communications to be issued by an executive branch official, rather than an independent member of the judiciary?
- What standard of proof should be required? Probable cause or an otherwise equivalent strong factual basis? Something else?
- What other protections should be required? Specificity as to the target, device, or account? Durational limits as to the scope of the request?

---

37. *See* Fed. R. Cr. Pro. 41(laying out in more specificity the standard for the issuance of criminal law warrants). The warrant standard for foreign intelligence collection is slightly different and not the topic of this article. *See* 50 U.S.C. §§ 1804-1805.

38. *See, e.g.*, Human Rights Council, Report of the Special Rapporteur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue, U.N. Doc. A/HRC/23/40, at ¶ 58 (Apr. 17, 2013); Human Rights Council, Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism, Martin Scheinin, U.N. Doc. A/HRC/13/37, at ¶ 50 (Dec. 28, 2009).

39. *See, e.g.*, 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; Daskal, *A New UK-US Data Sharing Agreement, supra* note 5.

- What kinds, if any, of emergency/exigent circumstances exceptions are acceptable?
- When is notice to the target required? In what circumstances can required notice be delayed, and for how long?
- What restrictions on access, dissemination, and retention are required?

A handful of court cases are beginning to flesh out some of these issues pursuant to regional human rights agreements.[40] But in general, human rights law – with its broad proclamations of the requirements that interferences of privacy be lawful, in pursuit of a legitimate aim, and necessary and proportionate – fails to provide the kind of granular answers to these questions that is needed.[41]

Complicating matters, even like-minded nations vary significantly in their respect for related free speech and associational rights. The United States' First Amendment guaranteeing the rights of speech and association provides particularly robust protections for such rights.[42] Few nations take such a speech-protective approach. This raises additional questions about harmonization of speech rights across borders. What kinds of speech-related prosecutions are justifiable, thereby supporting a request for data? That of the United States (as more rights-protective in this regard) or that of the requesting nation (presumably less rights-protective), assuming the requesting nation's laws and practices meets a baseline human rights standard? As is self-evident, the answers have profound implications for the global right to privacy, free expression, freedom of association, and other related rights.

---

40. *See, e.g.*, Davis v. Sec'y of State for the Home Dep't, [2015] EWHC (Admin) 2092 at ¶¶ 97-98, 114 (Eng.) (concluding that, pursuant to the Charter of Fundamental Rights of the European Union, as interpreted by the Court of Justice of the European Union, (CJEU) access to communications data requires prior review by a magistrate or independent administrative body). *But see* Sec'y of State for the Home Dep't v. Davis [2015] EWCA Civ 1185 at ¶¶ 113-115 (Eng.) (disagreeing with the lower court's analysis, concluding that related jurisprudence from the European Court of Human Rights considers prior independent review is "desirable" but not always necessary, and referring the case to the CJEU for further clarification). *See also* Ekimdzhiev v. Bulgaria, App. No. 62540/00, Eur. Ct. H.R. (June 28, 2007) at ¶ 90, http://hudoc.echr.coe.int/eng?i=001-81323 (concluding that notification to targets of surveillance is required once such surveillance has terminated and such notification can be made without jeopardizing the purpose of the surveillance").

41. The "necessary and proportionate principles," which have been signed by some 400 organizations and close to 300,000 individuals, are one attempt to elaborate these principles with more nuance, but they reflect an inspirational view of what the law should be, rather than a statement of current binding law. *See, e.g.*, ELECTRONIC FRONTIER FOUNDATION, *Necessary & Proportionate: International Principles on the Application of Human Rights Law to Communications Surveillance* 2 (2014), http://www.ohchr.org/Documents/Issues/Privacy/ElectronicFrontierFoundation.pdf (noting that "not all of the specific approaches we suggest have been formally or explicitly endorsed by international bodies for the protection of human rights").

42. Even in the United States, however, free speech rights have given way in the face of terrorism-related concerns. *See, e.g.*, Holder v. Humanitarian Law Project, 561 U.S. 1 (2010); David Cole, *The First Amendment's Borders: The Place of* Humanitarian Law Project *in First Amendment Doctrine*, 6 HARV. L. & POL'Y REV. 147 (2012).

Notably, the increasing interest in data across borders provides a human rights opportunity, at the same time it poses a risk. Specifically, the carrot of improved access to U.S.-provider-held data (which, at least for the time being constitutes the lion's share of the world's data) provides an opportunity for the United States to set a human rights and privacy-protective standard that governments must meet in order to make direct requests to U.S.-based companies for data – and get the expedited access that they want. Foreign governments (ideally) will be incentivized to participate in such a system – and meet the requisite substantive and procedural protections – because they, too, benefit from a harmonized system of access that minimizes conflict of law problems.

I discuss the delicate balance that must be struck and some proposed solutions in Part IV.

2. The Key Considerations: Non-Content

In general, non-content data receives significantly less protection than content data. This is due to the fact that the content of communications is considered more likely to reveal one's inner thoughts and is thus deemed more deserving of privacy protections than non-content data. But non-content data – what is sometimes called metadata or traffic data – also can provide an increasingly detailed account of one's interests, activities, and associations.[43] As we move toward what is known as an "Internet of Things" – with everything from our thermostats to our cars to our beds digitally connected – the quantity and quality of information revealed via so-called "non-content" data will continue to increase.[44]

Yet, as discussed above, there are few limits on government's cross-border access to such non-content data. Whereas U.S. law places stringent restrictions on foreign government access to content of stored data, it includes no analogous restriction on foreign government access to non-content data – including subscriber name and address, computer IP address, time and duration of session, and locational information. Other nations similarly fail to regulate access to such data.

The major U.S. providers now receive – and provide data in response to – tens of thousands of requests for such non-content data annually.[45] The companies assert that they take human rights concerns seriously, and, in fact, the major U.S. providers devote significant resources to the vetting of such foreign

---

43. *See, e.g.*, Daniel Solove, *Why Metadata Matters: The NSA and the Future of Privacy*, TEACHPRIVACY (Dec. 2, 2013), https://www.teachprivacy.com/metadata-matters-nsa-future-privacy.

44. *See, e.g.*, Paul Ohm, *Sensitive Information,* 88 S. CAL. L. REV. 1125 (2015); United States v. Jones, 132 S. Ct. 945, 954 (2012) (Sotomayor, J., concurring) (noting that non-content data obtained via GPS tracking can generate "a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations"); *Hearing on Continued Oversight of the Foreign Intelligence Surveillance Act Before the S. Comm. on the Judiciary*, 113th Cong. 3 (2013) (written testimony of Edward W. Felten, Professor, Princeton Univ.) (emphasizing the degree of personal information that can be gleaned about an individual simply by analyzing phone numbers called or received).

45. *See supra* note 22.

government requests. That said, the providers are operating without legal standards to guide them or even a set of best practices to apply. Moreover, requests are not only directed at the major companies that have the resources to engage in human rights vetting, but presumably made to a range of smaller providers and start-ups as well. Before Instagram was sold to Facebook in 2012, for example, it had just 13 employees.[46] To the extent it was receiving foreign government requests for data, it did not have a lot of extra capacity to evaluate such requests.

This matters for at least two reasons. *First*, it means private companies are being put in the position of determining the scope of users' privacy and related rights. And they are doing so without any domestic or international law rules or even a set of best practices to guide them.[47] While the major U.S. players appear to be expending meaningful resources in human rights vetting, there is no guarantee that this will remain a priority in the future – or that all future companies will be so inclined.

Second, whereas companies have incentives to be perceived as privacy and rights-protective (an incentive that is particularly strong for U.S. companies in the wake of the backlash following the Snowden revelations), they also face incentives cutting the other way. Foreign governments can, and do, threaten – and even arrest – locally based employees who fail to comply with their requests.[48] Foreign governments have the power to prohibit companies from doing business in their jurisdiction unless they comply with the requests for data. And foreign governments can otherwise exercise the power of the purse – limiting a

46. *See, e.g.*, Andy Baio, *Instagrams' Buyout: No Bubble to See Here*, WIRED (Apr. 10, 2012), http://www.wired.com/2012/04/opinion-baio-instagram-trend.

47. Whereas U.S. law imposes liability on companies that voluntarily disclose the content of communications unless specified conditions are met, there is no statutory prohibition on disclosure of non-content data to foreign governments. *See* 18 U.S.C. §§ 2702(a), (b) (2012). Moreover, even if the disclosed data is then used as a basis for abuse or harassment, it can be very difficult to trace back the data to its source. Furthermore, as private actors, companies are not directly bound by the ICCPR and most other treaty-based human rights obligations. In some very limited situations, actions of the private entities may be attributable to the state. In such a case, the state therefore can be held liable for the actions of their companies, and companies can be held to account for violations of privacy or other human rights as quasi-state actors. *See, e.g.*, Int'l Law Comm'n, *Draft Articles on Responsibility of States for Internationally Wrongful Act*, U.N. Doc. A/56/10, Supp. No. 10 (2001), [2001] 2 Y.B. Int'l L. Comm'n 32, U.N. Doc. A/CN.4/SER.A/2001/Add.1, art. 5 (describing situations in which the conduct of a person or entity shall be considered an act of the state based on their exercise of governmental authority) arts. 8-9 (explicating the situations in which the actions of a private party may be attributable to the state). But more often than not companies are deemed outside the reach of human rights law. And while the U.N. Human Rights Council has adopted Guiding Principles on Business and Human Rights, which impose obligations on corporations to respect and ensure human rights, these are neither specific as to how these private actors should handle law enforcement requests for data nor legally binding absent the adoption of national laws holding the private actors to account. Office of the High Comm'r. for Human Rights, *UN Guiding Principles on Business and Human Rights*, UNITED NATIONS (2011), http://www.ohchr.org/Documents/Publications/GuidingPrinciplesBusinessHR_EN.pdf.

48. *See, e.g.*, Kyle Wagner, *A Brief History of Google Employees Being Arrested in Foreign Countries,* GIZMODO (Sept. 27, 2012), http://gizmodo.com/5947043/a-brief-history-of-google-employees-being-arrested-in-foreign-countries.

range of highly sought-after government contracts with those that are willing to comply with their data demands.

All this points to the need for domestic and international law standards to guide the private actors that play such an important – and powerful role – in setting cross-border access to non-content data.

D. Jurisdictional Issues

Cross-border access to data also raises a set of critical questions about the relationship between territoriality and jurisdiction in an increasingly digitalized world. This section examines these issues via the lens of the recent Second Circuit decision regarding the reach of the United States' warrant authority under the Stored Communications Act.[49] It then shifts to the question of foreign government access to U.S.-held data, briefly describing the blocking provisions in U.S. law. It ends by suggesting an alternative approach to jurisdiction that turns on the location and nationality of the target, rather than the location of either the data or provider.

1. Microsoft Ireland – Warrant Jurisdiction

A recent case out of the Second Circuit – the so-called *Microsoft Ireland* case – highlights the key jurisdictional questions raised by law enforcement's interest in extraterritorially located data.[50] In that case the U.S. government sought data that is controlled by Microsoft, but held in Dublin, Ireland.[51] Microsoft refused to comply with the U.S.-court issued warrant on the grounds that the warrant authority extends only to the territorial borders of the United States; since the data was located in Dublin, the warrant had no force. But the magistrate and district court judge sided with the government. The data could be accessed and controlled from Microsoft employees operating within the United States. As a result, the exercise of the warrant was territorial, not extraterritorial – and valid.[52]

The Second Circuit reversed. According to the Second Circuit, the action sought by the government – that Microsoft retrieve data located in Ireland – was extra-territorial and thus outside the scope of the warrant authority. Congress had not explicitly authorized, let alone considered, the possibility that the statute at issue – the 30-year old Stored Communications Act (SCA) that had been passed when the Internet was in its infancy – would be used in this way; thus

---

49. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016).

50. *Id.* at 500-501.

51. *Id.*

52. *In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014); Brief for Appellee, *In re* Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985, at *9 (2d Cir. Mar. 9, 2015) (construing a Stored Communications Act warrant as a form of compelled disclosure, akin to a subpoena, under which the location of the provider controls).

the presumption against extraterritoriality kicked in. The government could not, according to the Second Circuit, rely on the statute to compel the production of data located outside the United States.

There are several interesting aspects of the case.[53] For our purposes, the most important is the Second Circuit's determination that the location of the data – rather than the location of the provider accessing the data – was the key determinant of territoriality, and thus jurisdiction. Consider the implications: Pursuant to this ruling, the U.S. government has jurisdiction over data held within the United States territorial jurisdiction, whereas the Irish government controls access to data within the territory of Ireland. If the United States wants data located in Dublin, it now needs to make a diplomatic request for the data – just as the United States would demand if Irish law enforcement sought data held in the United States.[54]

The result is concerning; although I would have said the same if the government had won. As I explain in what follows, both sides' positions were unsatisfactory. The location-of-data rule adopted by the Second Circuit provides a strong incentive for mandatory data localization as a means of controlling governmental access to sought-after data. Companies could seek to evade the U.S. government's reach simply by moving communications data elsewhere, and governments could mandate that they do so in order to retain control. This has negative consequences for the innovative potential of the Internet and for privacy rights of both American and foreign-based users. After all, the U.S. requirement that law enforcement officials obtain a warrant issued by a neutral magistrate based on a standard of probable cause before accessing the content of stored communications is as high of a standard as one will find anywhere. Data localization mandates are likely to result in foreign governments being able to compel the production of data – including of Americans – based on a much lower standard than what would apply if the data were sought by the United States.

Additional security-based and normative problems also result from such an approach, pursuant to which enforcement jurisdiction turns on where data

---

53. While often described as a "privacy case," that label does not accurately describe the key issue in dispute. *See, e.g.*, Mark Scott, *Ireland Lends Support to Microsoft in Email Privacy Case*, N.Y. TIMES (Dec. 24, 2014), http://bits.blogs.nytimes.com/2014/12/24/ireland-lends-support-to-microsoft-in-email-privacy-case (describing the dispute a "privacy case"). The United States, after all, is proceeding based on a warrant issued by a U.S. magistrate based on a finding of probable cause. It would not be a privacy violation to compel production of the data if it were stored in the United States. It thus does not become an infringement on privacy simply because the data is stored in Ireland. The case, however, does raise important questions about enforcement jurisdiction, territoriality, and sovereignty – issues that have *implications* for privacy rights. The issue is about who does – and should – control access to the data in such a situation: State A, State B, or both? It is thus a question about who sets the rules, and hence the applicable privacy and related human rights protections.

54. For interested readers, I highly recommend Judge Lynch's concurring opinion in the case, which does a phenomenal job of summarizing the key issues and explaining the need for Congressional action. *See In re* Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No.14-2985 (2d Cir. July 14, 2016) (Lynch, Circuit Judge, concurring).

happens to be located at any given moment.[55] Imagine, for example, a U.S. agent investigating a New York murder. Imagine further that law enforcement agents obtained a warrant based on probable cause ordering Microsoft or any other U.S.-based Internet Service Provider to disclose emails sent to or from the alleged perpetrator around the time of the murder. Under the Second Circuit's ruling, the agents could compel such production *if* the data were stored in the United States. But it would have to make a diplomatic request for the data if it were stored in another nation's territory. This makes little sense, and could have significant security costs – as well as privacy costs, given that most other nations will apply a weaker privacy-protective standard than the United States to the accessing of the data. Moreover, as a practical matter, the rapid mobility and divisibility of data makes data location a highly unstable basis of jurisdiction.

And as a normative matter, a jurisdictional rule that turns on data location often seems arbitrary. After all, when one stores data in the cloud, one often has no idea – and no control – over where his or her data is held at any given moment; the same is true with respect to the multitude of information shared via apps on our phones or tablets.[56] Why, then, should government access to one's data depend upon where the data happens to be stored – particularly if the user does not know and has no role in choosing that location?[57]

Conversely, the government's position also raises concerns. The United States argued in the case – and will likely argue in further cases and before Congress[58] – that it should be able to compel the production of data, wherever located and without regard to the nationality or location of the target, so long as it has jurisdiction over a provider that can access the data. It conceded that the same approach would apply if Germany sought to compel the production of a U.S. citizen's data held by a German-based provider on U.S. soil; it could do so, so long as the German government complied with German process.[59] This may not seem so concerning when dealing with a U.S.-based or German-based provider and it is the United States or German government doing the compelling. But this same claim is not, and will not, be limited to these governments.[60]

---

55. *See, e.g.*, Jennifer Daskal, *Three Key Takeaways: The 2d Circuit Ruling in the Microsoft Case,* JUST SECURITY (July 14, 2015), https://www.justsecurity.org/32041/key-takeaways-2d-circuit-ruling-microsoft-warrant-case; Daskal, *The Un-Territoriality of Data*, *supra* note 5.

56. It is of course conceivable that users could enter contracts requiring data be stored in specific locations, but at least currently the average user does not do so; it also would add significant inefficiencies – and costs – into the system if providers could no longer freely move data across territorial boundaries because of restrictions imposed by their consumers.

57. *See* Daskal, *The Un-Territoriality of Data, supra* note 5, at 365-377, 379-396 (making this argument in much more detail).

58. The U.S. government plans to seek legislation to explicitly grant law enforcement officials the authority to compel the production of data that is located extraterritorially *See* Letter from Peter J. Kadzik, *supra* note 15.

59. Transcript of Oral Argument at 55, *In re* Warrant To Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., No. 14-2985-CV (2d Cir. Mar. 9, 2015).

60. The United States is, after all, not the only nation to assert such broad authority to compel the production of data. *See, e.g.*, Winston Maxwell & Christopher Wolf, *A Global Reality: Government*

Moreover, the central premise – that as long as the state has jurisdiction over the provider it can compel production over sought-after data – arguably justifies any country in the world with jurisdiction over any provider (including US-based providers) from compelling, according to their own standards, access to sought-after data. One can easily conceive of a law enforcement free-for-all. Nations assert the authority to compel ISPs, cloud-based service providers, and app providers that do business in their jurisdiction to produce sought-after data, regardless of other considerations, such as the location of the target, citizenship of the inquiry, and strength of the state's interest in the data. Some may do so based on a warrant (or its equivalent) and a finding of probable cause (or its equivalent) that the data contains evidence of a particular crime. But others may seek the data as a basis for keeping tabs on political opponents or suppressing dissent, with minimal to no procedural and substantive safeguards in place.[61]

One of two possible scenarios would likely emerge. (There are of course more, but these two highlight the basic concerns.) One is that nations – including the United States – would have little to no say about when, for what reasons, and pursuant to what procedural and substantive safeguards, their own citizens' data could be collected by foreign governments. This would almost certainly yield a race to the bottom with respect to privacy, with individuals having little to no ability to safeguard their data from foreign government requesters unless they exclusively relied on locally-based providers that lacked any international presence – a near-impossibility in the modern, interconnected world.

Alternatively (and in response), national legislatures would reject this state of affairs and adopt additional blocking statutes designed to protect their residents' and citizens' data. Such blocking provisions would prohibit providers that do business in their jurisdiction from responding to foreign-based requests for such data, and instead require the exercise of formal government-to-government requests for data. But this would simply exacerbate the conflict of laws problems that exist. One nation would compel the production of data, and another would prohibit it, putting companies in the untenable position of having to choose which laws to comply with and which to violate. Nations would likely vie to impose the heftiest penalties – or alternatively to promise the biggest benefits – so as to incentivize compliance.

While some may suggest that such conflict of law problems are not new, and simply the cost of doing international business, that seems to me an unsatisfactory answer. Simply because companies have faced competing regulatory or enforcement burdens elsewhere does not mean one should recreate these problems with respect to law enforcement access to data. Among other problems, such a result would make it increasingly difficult for smaller start-ups to operate

---

Access to Data in the Cloud (Hogan Lovells 2012), http://www.cil.cnrs.fr/CIL/IMG/pdf/Hogan_Lovells_White_Paper_Government_Access_to_Cloud_Data_Paper_1_.pdf.

61. More cynically, one can imagine law enforcement officials in a state with strong privacy protections relying on a foreign partner to compel production of sought-after data as an end-run around their own restrictions on access.

globally, with negative costs to the innovative potential of the Internet. A system of multiple, competing laws would also impose security costs, as nations would face increased difficulties in gaining timely access to data that is subject to overbroad blocking provisions imposed by a foreign partner.

2. The U.S. Blocking Provisions

At the same time that the United States executive branch has been asserting the extraterritorial reach of the U.S. warrant authority in the Microsoft Ireland case, the United States explicitly prohibits foreign governments from doing the same with respect to U.S.-controlled communications content. This is due to a provision in the SCA that prohibits, albeit with some exceptions, the disclosure of certain stored content, including emails, to anyone other than the U.S. government pursuant to a U.S.-judge issued warrant based on the U.S.-based standard of probable cause.[62] It thus bars companies from being able to respond to foreign government requests for the content of communications, even in situations where the foreign government has complied with its domestic legal requirements and is seeking the data of one of its own citizens in connection with the investigation of a local crime.

While the provision is silent as to its reach, it has been interpreted by several companies as applying to all data under its control. Google and Facebook, for example, assert that they are bound by the provisions of the SCA and thus broadly prohibited from turning over the content of stored communications to foreign-based providers, regardless of the location of the sought-after data at any given moment in time.[63] Microsoft, by contrast (and consistent with its approach in the Microsoft *Ireland* litigation described above) appears to take the position that the location of data is what controls. According to this view, a company could not disclose U.S.-held data to foreign governments, but could respond to foreign government requests for extraterritorially-located data.[64]

---

62. 18 U.S.C. §§ 2702(a), (b) (2015) prohibit the disclosure of the content of communications, subject to certain exceptions. Pursuant to §§ 2703(a), (b), a "governmental entity" may compel production of the content of communications pursuant to a warrant based on probable cause, but, as described *supra* note 21, "governmental entity" is defined as a "department or agency of the United States or any State or political subdivision thereof" under § 2711(4). There is no legal basis for foreign governments to directly compel production of content. Moreover, although the requirement of a warrant based on probable cause only applies to certain types of providers and to communications held for 180 days or less, the Sixth Circuit in *United States v. Warshak*, 631 F.3d 266 (6th Cir. 2010), held that the warrant requirement governs the compelled disclosure of emails regardless of how long they have been stored; current U.S. executive branch practice is to obtain a warrant when it seeks the production of emails, irrespective of the time of storage or categorization of provider.

63. Conversely, Google argues that it is, as a result, not subject to the regulatory jurisdiction of others. Christopher Williams, *Google Argues UK Privacy Laws Do Not Apply to It*, TELEGRAPH (Aug. 18, 2013), http://www.telegraph.co.uk/technology/google/10250801/Google-argues-UK-privacy-laws-do-not-apply-to-it.html (noting Google's assertion that it is not subject to the regulatory jurisdiction of the UK because the relevant services are provided by Google Inc., based in California).

64. Microsoft's argument centers on the claim that the United States should employ mutual legal assistance tools in order to have access to the data. Under this approach, Ireland would access the data pursuant to its own processes (including any relevant privacy regulations) and then turn it over to the

Regardless of the approach, the blocking provision is causing increasing frustration on the part of foreign governments seeking U.S.-held or U.S.-controlled data in the investigation of local crime. It is incentivizing the kind of dangerous responses discussed in Part I, including the imposition of mandatory data localization requirements, unilateral assertions of jurisdiction, and the use of other surreptitious means of accessing sought-after data.

III. THE WAY FORWARD: CONTENT DATA

The need for new – and agreed upon – cross-border mechanisms that facilitate law enforcement access to the content of communications in a manner that respects the multiple human rights, security, and economic interests at stake is only going to increase over time. Three things seem clear:

First, doing nothing is not a preferred solution. Inaction will almost inevitably lead to increased claims of unfettered access; employment of other, more covert means of gaining access to sought-after data and increased demands for forced data localization as a means of preserving government access to such data. *Second*, design of a new system is not going to be easy. *Third*, and relatedly, the problem presents an opportunity as much as it presents a challenge. If done right, it can provide an incentive for countries to raise protections and set rules where few currently exist. But it also poses difficult questions about the substantive and procedural baselines required, the ways in which the collected data can be used, and standards for accountability. While human rights law can and should shape the considerations brought to bear on the design of new cross-border data sharing agreements, it is not going to provide the kind of granular direction needed in this area. To the contrary, the design of such agreements is likely to shape the scope of, and to some extent the framework for evaluating, human rights protections in this area. The remainder of this section addresses both framework design and the substantive features of what such agreements should include.

A. A New Treaty?

Some have suggested that what is needed is a new international instrument, such as a treaty, that would establish some sort of supranational warrant system based on globally applicable substantive and procedural requirements for the access of data.[65] But while there are obvious advantages to an internationally agreed-upon system for cross-border access, this is more of a textbook solution than something that could realistically be put in place, at least in the short-term.

United States. Implicit is the assumption that governments have enforcement jurisdiction over data within their territorial jurisdiction, but that such jurisdiction does not extend to data located beyond that nation's territorial borders.

65. *See, e.g.*, Brad Smith, *Time for an International Convention on Government Access to Data,* DIGITAL CONSTITUTION BLOG (Jan. 20, 2014), http://digitalconstitution.com/2014/01/time-international-convention-government-access-data.

Among the many potential problems, any attempt to reach international agreement is likely to yield a retreat to the lowest common denominator, and thus a watering down of the procedural and substantive protections that would otherwise apply in many nations, including the United States.

B. The Less Ambitious Approach: The U.S.-U.K. Model

A better approach would be to start small, ideally as a set of bilateral or multilateral agreements among a handful of like-minded countries.[66] Rather than develop new internationally agreed upon standards and institutions, relatively like-minded nations would identify a set of baseline jurisdictional principles, as well as substantive and procedural standards that operate as pre-conditions for being permitted to directly compel the production of foreign-held data. This would begin to set a framework that could then be adopted by others.

Notably, the United States and United Kingdom currently are seeking to negotiate just such an agreement, pursuant to which jurisdiction turns on the location and nationality of the target, rather than the location of the data. Under the terms currently being discussed, U.K. law enforcement officials would be permitted to directly request the content of communications of targets that reside outside the United States, and are not U.S. citizens or legal permanent residents.[67] (U.S. law enforcement would be permitted to make direct requests to U.K.-based service providers under similar terms.)[68] If, however, the U.K. sought emails of U.S. citizens, legal permanent residents, or persons residing in the United States regardless of their nationality, it would not be able to make direct requests to the providers. As is currently the case, that data could only be produced based on the issuance of a U.S. warrant pursuant to a U.S.-based standard of probable cause.[69]

Such a demarcation reflects the principles that U.S. standards should continue to govern access to data of U.S. citizens, legal permanent residents, and persons located within the United States – whereas the United States has little justification in imposing these specific standards on foreign government access to data of non-citizens who are located outside the United States. Similarly, U.K.

---

66. *See* Jennifer Daskal & Andrew K. Woods, *A New UK-US Data Sharing Treaty?*, JUST SECURITY (June 23, 2015), https://www.justsecurity.org/24145/u-s-u-k-data-sharing-treaty; Stephen Schulhofer, *An International Right to Privacy? Be Careful What You Wish For* 26-27 (N.Y. Univ. Pub. Law & Legal Theory Working Paper, Paper No. 508, 2015), http://lsr.nellco.org/cgi/viewcontent.cgi?article=1511&context=nyu_plltwp (advocating reliance on reciprocal, bilateral relationships – what he calls "bilateral parity").

67. *See Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests Before the H. Comm. on the Judiciary*, 114th Cong. 8, 10 (2016) (statement of David Bitkower, Principal Assistant Deputy Attorney General, Department of Justice) [hereinafter *Bitkower Statement*].

68. *See id.* at 10.

69. Such data could not be produced at all if the UK were seeking live, as opposed to stored, communications – absent the initiation of a joint investigation.

standards should govern access to data of U.K. citizens, legal permanent residents and persons located within the U.K. – but the U.K. has little justification imposing these specific standards on foreign government access to data of non-U.K. nationals located outside the United Kingdom.

Such an agreement could help to minimize the dangerous incentives in favor of mandatory localization, unilateral assertions of extraterritorial jurisdiction, and mandatory decryption requirements.[70] As the first of its kind, it would also become a model for other agreements, thus helping to set more broadly applicable standards governing cross-border access to data.[71]

This, however, also suggests the need to proceed with care – both as to the design of the process and the specific procedural and substantive requirements that are demanded.

C. The Role for Congress

The kind of agreement being negotiated between the United States and United Kingdom cannot be implemented by the executive branch alone. Congress needs to first amend the Stored Communications Act to lift the prohibition on U.S.-based providers disclosing the content of communications to foreign officials. A separate amendment to the Wiretap Act would be required to permit direct access to real-time communications.[72] Congress thus has a unique opportunity to authorize the executive to both enter into the kind of agreements being contemplated with the U.K. and define the baseline substantive and procedures standards that should apply. It should seize this opportunity while it can.

Specifically, Congress should authorize the executive to enter into bilateral and multilateral agreements, pursuant to which foreign governments could directly compel the production of sought-after data from U.S.-based providers, so long as the target of the request is a not a U.S. citizen or legal permanent resident, and is not located in the United States.[73] Congress should also *set the key parameters of such agreements* – ensuring among other things that foreign governments continue to rely on the MLA system (including the requirement of a warrant based on probable cause) to get the data of U.S. residents, as well as

---

70. *See* Daskal, *A New UK-US Data Sharing Agreement*, *supra* note 5.

71. *See also Bitkower Statement*, *supra* note 69, at 10 ("If the approach [being discussed between the United States and United Kingdom] proves successful, we would consider it for other like-minded countries as well.").

72. The wiretap provisions require additional consideration, given, among other things, the more rigorous court review and minimization requirements that have been applied to wiretaps than access to stored communications under U.S. law. That said, the line between stored communications and live intercepts is increasingly blurring, and the same principles that justify permitting expedited access to stored content seem to also apply to live intercepts, providing sufficient protections are put in place. *See Hearing on International Conflicts of Law Concerning Cross Border Data Flow and Law Enforcement Requests Before the H. Comm. on the Judiciary*, 114th Cong. 8 (2016) (statement of Jennifer Daskal, Assistant Professor) (addressing additional considerations posed by live intercepts).

73. This could be done by adding a new exception to the blocking provisions in the SCA that would authorize providers to disclose the content of communications to foreign governments pursuant to the terms of any bilateral and multilateral agreements negotiated by the executive branch.

U.S. citizens and legal permanent residents wherever located. It should also require that the requesting country meets basic human rights standards; that the particular requests satisfy a baseline set of procedural protections; and that the system is subject to meaningful transparency and accountability mechanisms.

The following elaborates on these requirements in more detail:

(i) *General Human Rights Protections*: The executive branch should be required to certify that the partner government laws and practices meet basic human rights norms, including, for example, compliance with the prohibition against torture and other cruel, inhuman, and degrading treatment of persons within the state's custody or control; provision of basic fair trial rights; and protection of the right to free expression. This is critical to guard against sought-after data being used to torture, abuse, or otherwise violate the target's (or others') human rights.

(ii) *Request-Level Protections:* The legislation should specify a set of baseline requirements that the requests made under this system should meet. These should include, at a minimum, a requirement that the requests be made by an independent and impartial adjudicator; be targeted to a particular person, account, or device; be narrowly tailored as to duration; and be subject to effective minimization requirements to protect against the retention and dissemination of non-relevant information.

(iii) *Transparency and Accountability Measures*: The legislation should mandate that the partner government publish reports regarding the number, type, and temporal scope of the data requests they issue under this framework. (The United States should similarly agree to do the same with respect to requests made of foreign-based providers.) Governments should also be required to comply with assessment mechanisms that evaluate compliance with these requirements.

(iv) *Sunset Provision*: The legislation should specify that any such agreement sunset after a set period of years, absent an assessment that the requisite procedural and substantive requirements have been met.

These requirements are essential and justified under U.S. law for at least two key reasons. *First,* while the targets of foreign government requests under this system will be foreign nationals that are located outside the United States, communications are inherently intermingled. It is likely – in fact almost certain – that such requests will at times lead to the incidental collection of U.S. citizen data and data of other persons physically residing in the United States. This reality provides both an opportunity, and arguably an obligation, for Congress to demand a minimal set of baseline standards to protect those persons that fall squarely within its responsibility and authority to protect. Other nations similarly have such responsibility and authority with respect to their own nationals and residents.

Second, by dint of U.S. control over both the relevant providers and the data they control, the U.S. has a unique opportunity to set the standards that apply. The United States is often in the position, via its annual State Department Human Rights reporting and myriad other diplomatic channels, of exhorting other countries to improve human rights standards and protect the right to free expression. The United States now has a rare opportunity to couple such exhortations with a potentially attractive carrot – expedited access to U.S.-controlled data. These incentives allow for the leveling up, rather than the leveling down, of protections for all – and put the United States in the position of helping to shape privacy norms both within and outside its borders. At the same time, it will be helping to minimize conflicts of laws and promote the development of an open (not Balkanized) Internet.

Notably, legislation proposed by the Department of Justice, and recently transmitted to Congress, incorporates each of these key elements. While there is room to improve on some of the details, the general approach is one to be applauded. It requires the Attorney General, in conjunction with the Secretary of State, to certify that the partner government affords "robust substantive and procedural protections for privacy and civil liberties;" includes numerous request-level requirements, including that the requests be targeted, of limited duration, and not used to infringe free speech; prohibits the intentional targeting of persons located in the United States or U.S. citizens and legal permanent residents, wherever located; prohibits the dissemination of non-relevant information; and includes a five-year sunset, absent an executive branch determination that the criteria are being met. It is legislation that Congress should take up and ultimately adopt, ideally with some increased transparency and accountability mechanisms, among other improvements.[74]

D. The Critiques

The design of a system to govern law enforcement access to data across borders is difficult, and no solution is perfect. This proposal is no exception. The following addresses and responds to some of the most salient criticisms of such an approach.

Some warn that this framework will lead to the "elimination" of the probable cause requirement in a way that will undercut key privacy protections.[75] Put another way, the relative robustness of U.S. substantive and procedural require-

74. *See* Legislation to Permit the Secure and Privacy-Protective Exchange for Electronic Data for the Purposes of Combating Serious Crime Including Terrorism in Letter from Peter J. Kadzik, *supra* note 15. *See also* Melanie Teplinksi & Jennifer Daskal, *Opinion: How the Justice Department data-sharing plan defends privacy,* CHRISTIAN SCI.MONITOR, July 27, 2016, http://www.csmonitor.com/World/Passcode/Passcode-Voices/2016/0727/Opinion-How-the-Justice-Department-data-sharing-plan-defends-privacy; Daskal & Woods, *Cross-Border Data Requests*, *supra* note 5.

75. *See, e.g.*, Greg Nojeim, *MLAT Reform Proposal: Eliminating U.S. Probable Cause and Judicial Review*, LAWFARE (Dec. 4, 2015), https://www.lawfareblog.com/mlat-reform-proposal-eliminating-us-probable-cause-and-judicial-review.

ments means that the United States should continue to insist on a U.S. warrant and probable cause standard whenever foreign governments seek the content of communications from U.S.-based providers; after all, such a requirement provides a critically important protection for U.S. citizens and non-citizens alike.

But this critique assumes a world that does not exist. It assumes that foreign governments will comply with the existing diplomatic procedures for accessing sought-after data rather than seeking out means of accessing the data unilaterally – whether via data localization requirements, unilateral assertions of extraterritorial jurisdiction, or use of malware or other surreptitious means of accessing the data. For all the reasons described in Part I, nations are instead being incentivized to find ways around these diplomatic procedures and seek out these other means of accessing sought-after data. Such measures enable domestic surveillance based on foreign government's own domestic practices – practices that in many places do not require warrants or anything like probable cause, and, in some cases, fail to meet even baseline human rights protections. At some point, these alternative means of accessing data will be entrenched, and the United States' leverage with respect to the standards that apply will be lost.[76]

Others have critiqued the proposed approach on the grounds that, even if the suggested framework is adopted, only a fraction of foreign governments will meet the specified requirements, and thus only a fraction of foreign governments will be in a position to enter into these types of agreements. The most repressive nations – and thus the nations we ought to be most concerned about – are not going to be in a position to meet the applicable requirements any time soon, at least absent significant changes to their systems. As a result, nations such as China, Russia, and Iran, and many others, will continue to pursue the very set of localization requirements, claims of unilateral access, and use of other measures to access data that this approach is seeking to prevent.[77]

That is a fair point. But the fact that this framework will not be a panacea for all potential problems does not mean it should be abandoned altogether. There are, after all, a number of countries that will continue to disregard privacy rights no matter what the United States does. But there are also a number of nations – like the United Kingdom and several others – that are interested in and willing to adopt reciprocally binding rules governing cross-border access to data so as to both facilitate increased access to sought-after data and minimize cross-border conflicts over such data. The United States should seize this

76. It is, of course, impossible to determine with certainty both the extent to which governments will take measures to facilitate such surveillance and the degree to which any particular solution will minimize these incentives. But it is a mistake to assume that the current U.S. standards do – and will continue – to provide broad-based privacy protections vis-à-vis foreign governments seeking access to U.S.-held data, and that therefore any change to such standards constitutes a watering down of privacy protection that would otherwise apply.

77. *See Bitkower Statement supra* note 69, at 8 (emphasizing that only "like-minded nations" would be in the position to enter into the kind of agreement currently being negotiated with the United Kingdom); Krishnamurthy, *supra* note 9, at 12 (emphasizing that countries like China and Russia are not likely to benefit from any such agreement any time soon).

opportunity. Even if only a handful of countries participate initially, such an approach is a start. It alleviates conflicts with those countries and begins to set the stage for a broader approach to cross-border access to data in ways that simultaneously promote privacy, security, and the growth of the Internet.

Yet another critique accepts the premise of the project, but objects to the focus on location and nationality of target as the key criteria for determining foreign government access to the data. There are two variants of this critique: one practical and one normative. On the practical side, several commentators have noted the difficulty with determining target location and nationality – a key requirement under the proposed framework. Foreign governments simply will not have that information in many cases.[78] In the absence of knowledge, governments will be required to adopt a series of presumptions, relying on things like IP addresses as a proxy for determining location and perhaps even nationality.[79] But such presumptions are hardly foolproof. Users can hide or conceal their actual IP address. And even if the target's IP address accurately reveals location, it simply tells us about the target's location at a given point in time (or several points in time), and is not a particularly accurate indicator of either nationality or immigration status. Put simply, any presumption, whether based on IP address or something else, will yield both false positives and false negatives. As a result, foreign governments will be getting direct access to U.S. person data based on their own standards when they should be employing the MLA system, replete with the protections of a warrant and probable cause. Conversely, it may lead foreign governments to rely on the MLA system when, in fact, they could have obtained the data directly from the companies – although that tends not to be high on the list of most critics' concerns.

But while this is also a valid critique, a jurisdictional test that turns on user nationality and location still appears to be the best, albeit imperfect, means of promoting harmonization across national borders. Consider the two most likely alternatives: data location or provider location as the basis for enforcement jurisdiction. Both create more problems than they solve. Reliance on data location is unpredictable, manipulable, and normatively troubling– as the location of one's data may not have any relationship to either the user's physical

78. *See, e.g.*, Krishnamurthy, *supra* note 5, at 12 (noting the practical difficulties with such an approach).

79. There is precedent for this. The statutory rules governing foreign intelligence surveillance in the United States similarly require an assessment of target nationality and location; the intelligence agencies must make "foreignness" determinations prior to targeting. The NSA has adopted a "totality of the circumstances" test that has, at least according to one audit, resulted in a high degree of accuracy. PRIVACY AND CIVIL LIBERTIES OVERSIGHT BOARD, REPORT ON THE SURVEILLANCE PROGRAM OPERATED PURSUANT TO SECTION 702 OF THE FOREIGN INTELLIGENCE SURVEILLANCE ACT 43-45 (July 2, 2014), https://www.pclob.gov/library/702-Report.pdf (describing that a DOJ audit of 2011 NSA data found an error rate of just 0.4%); *Public Hearing Regarding the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act Before the Privacy and Civil Liberties Oversight Bd.* 40-41 (Mar. 19, 2014), http://www.pclob.gov/library/20140319-Transcript.pdf. That said, the NSA is likely to have much more information at its disposal on any given target than most foreign law enforcement; one would thus expect the error rate for law enforcement to be higher.

location or the underlying activity that is triggering the criminal justification. A jurisdictional test that turns on data location also further incentivizes data localization, with negative consequences for privacy, security, and the growth of the Internet.

A jurisdictional test based on provider location provides more stability than a test based on data location but comes with other costs. Such a test fails to resolve the key conflict of law problems that this framework is intended to address. Providers that operate across state lines will continue to be subject to multiple, and often competing, claims of jurisdiction. And while such conflict problems could be avoided by a test that focuses exclusively on where the provider is either headquartered or principally operates, this too is subject to manipulation. More importantly, it does little to solve the underlying, normative frustration that has triggered the concerns in the first place: Why should U.S., U.K., or any other government's access to emails on one of its own citizens in the investigation of a local crime turn on where the citizen's email provider is headquartered? There is no good answer to that question.

Others complain that a jurisdictional test that focuses on nationality and location is "NIMBY-like" in that it carves out protections for a nation's own citizens, legal permanent residents, and denizens, but permits third party nationals' data to be collected based on the (presumably) lower standards applied by requesting foreign governments.[80] This critique is analogous to the concern about the so-called "elimination" of the probable cause standard. It is premised on the idea that the United States, in reserving the probable cause standard for U.S. citizens, legal permanent residents, and persons located in the United States, is leaving third party nationals out to dry, subject to the whims of foreign government requesters. But by setting baseline procedural and substantive standards that foreign partners must meet, this framework actually raises, rather than lowers, privacy protections as compared to the status quo. Consider again the incentives laid out in Part I. As foreign governments increasingly succeed in their imposition of mandatory data localization requirements, unilateral assertions of extraterritorial jurisdiction and/or reliance on other surreptitious means of accessing sought-after data, they will be able to access sought-after data based on their *own* standards, without any requirement that they adopt baseline procedural and substantive standards in order to do so. The framework suggested here, by contrast, permits foreign governments to access sought-after data – including that of foreign nationals – but imposes a set of baseline substan-

80. Gidari, *MLAT Reform*, *supra* note 5. Under Gidari's approach, expedited access to U.S.-held data would be permitted only in the very narrow set of cases where there is a finding of dual criminality and *all* parties to the crime (including witnesses) are within the territorial jurisdiction of the requesting state. But while this is an interesting approach, it is not likely to sufficiently satisfy the foreign government interest in data located outside its borders – and will thus insufficiently protect against the negative incentives laid out in Part I.

tive and procedural protections than must apply.[81]

The growing interest in access to data across borders provides a human rights opportunity, at the same time it poses a risk. Specifically, the carrot of improved access to U.S.-provider held data (which, at least for the time being, represents the lion's share of the world's data) provides an opportunity for the United States to set a human rights floor that governments must meet in order to make direct requests to U.S.-based companies for data – and get the expedited access that they want. If done right, foreign governments will be incentivized to participate in such a system – and meet the requisite substantive and procedural protections – because they, too, benefit from a harmonized system of access that minimizes conflict of law problems.

Importantly, the U.S. leverage to demand these basic substantive and procedural requirements will not last forever. Currently, foreign governments still have an incentive to participate in such an agreement because they, too, benefit from harmonization of the relevant jurisdictional rules. At some point, however, data localization may become entrenched and the Balkanization of the Internet so great that the incentive to enter into these types of agreements will no longer exist. At that point, local rules will reign, without any of the baseline protections that this framework seeks to require.

E. Non-Content Data

Currently, as described above, U.S. law imposes no standards with respect to requests for non-content data from foreign-based governments. This should change. Consistent with the jurisdictional approach advocated for content, the United States ought to set baseline standards governing foreign government requests for certain non-content data of persons located within the United States, as well as U.S. citizens and residents wherever located. At a minimum, it seems, foreign governments should be subject to equivalent standards as to those the United States is obliged to meet when it seeks the kinds of non-content data (such as to/from lines on emails) that is subject to heightened protections under U.S. law – namely a showing of "specific and articulable facts showing that there are reasonable grounds to believe that the . . . records or information sought are relevant and material to an ongoing criminal investigation."[82]

---

81. Vivek Krishnamurthy additionally raises questions about situations of dual citizenship. He notes, for example, the anomaly that would result if the Canadian government could not, in the investigation of local crime, directly access a Canadian resident's data simply because he holds dual Canadian-American citizenship and the data was held by a U.S.-based provider. Krishnamurthy, *supra* note 5, at 12. Such a critique highlights the inevitable problems with any type of line drawing. It is always possible to identify a range of instances where the line seems arbitrary, unfair, or even contrary to the intended purposes. And if in fact that category of cases is sufficiently large to pose a significant concern, one could adopt a provision to deal with it – such as a separate set of rules for cases involving dual nationality. But the critique is not fatal to either the project or the specific approach proposed here.

82. 18 U.S.C. § 2703(d). Specifically, I propose amending 18 USC § 2702(a) to specify that a provider of electronic communication service or remote commuting service shall not knowingly

Informal conversations suggest that such a standard is largely consistent with what the major U.S. providers are already requiring. It would, as a result, enshrine good practices without imposing a major burden on such providers. And it would ensure that new entrants to the market similarly hold foreign governments to this minimal standard before it accesses the kind of non-content data that can reveal a target's movements, associations, and activities. It also has the advantage of giving the providers a specific requirement to point to as grounds for rejecting foreign government requests – thus potentially making them better able to resist both subtle and more overt pressures to comply.

Corporations also ought to be required to report on the number and type of such requests received and complied with. Most major U.S.-based providers already produce such transparency reports voluntarily. It would be helpful to enshrine this practice in law – and to mandate increased detail about the nature of the requests, including the kind of data sought and the duration of the requests.

Both of these changes can be done via simple amendments to the Stored Communications Act – and would, as with the proposed agreements for stored content – begin to set standards that would ideally be adopted by others.

CONCLUSION

As data has become increasingly global, the interest of law enforcement has followed. We are now seeing a surge of cross-border requests for data. Blocking provisions in U.S. law are causing a backlash – resulting in countries seeking to unilaterally bypass these restrictions and/or demand that data be stored locally so as to avoid the U.S.-based legal restrictions on the sharing of sought-after data. This has negative consequences for security, privacy, and the future of the Internet. Meanwhile, few rules govern the sharing of non-content data. Corporations are increasingly put in the position of vetting these requests, but without any clear conclusions to fall back on. The situation demands our increased attention – to facilitate the legitimate law enforcement access to data; guard against the creation of a Balkanized Internet; promote harmonization of rules across jurisdictions; and protect privacy.

---

divulge a record or other information (not including the records specified in § 2703(c)(2)(A)-(F) and not including contents of communications covered by paragraph (1) or (2)) pertaining to a subscriber to or customer of such service who is a U.S. person or person located in the United States to any foreign government official unless the request includes specific and articulable facts showing that there are reasonable grounds to believe that the records or information sought are relevant and material to an ongoing criminal investigation.

***