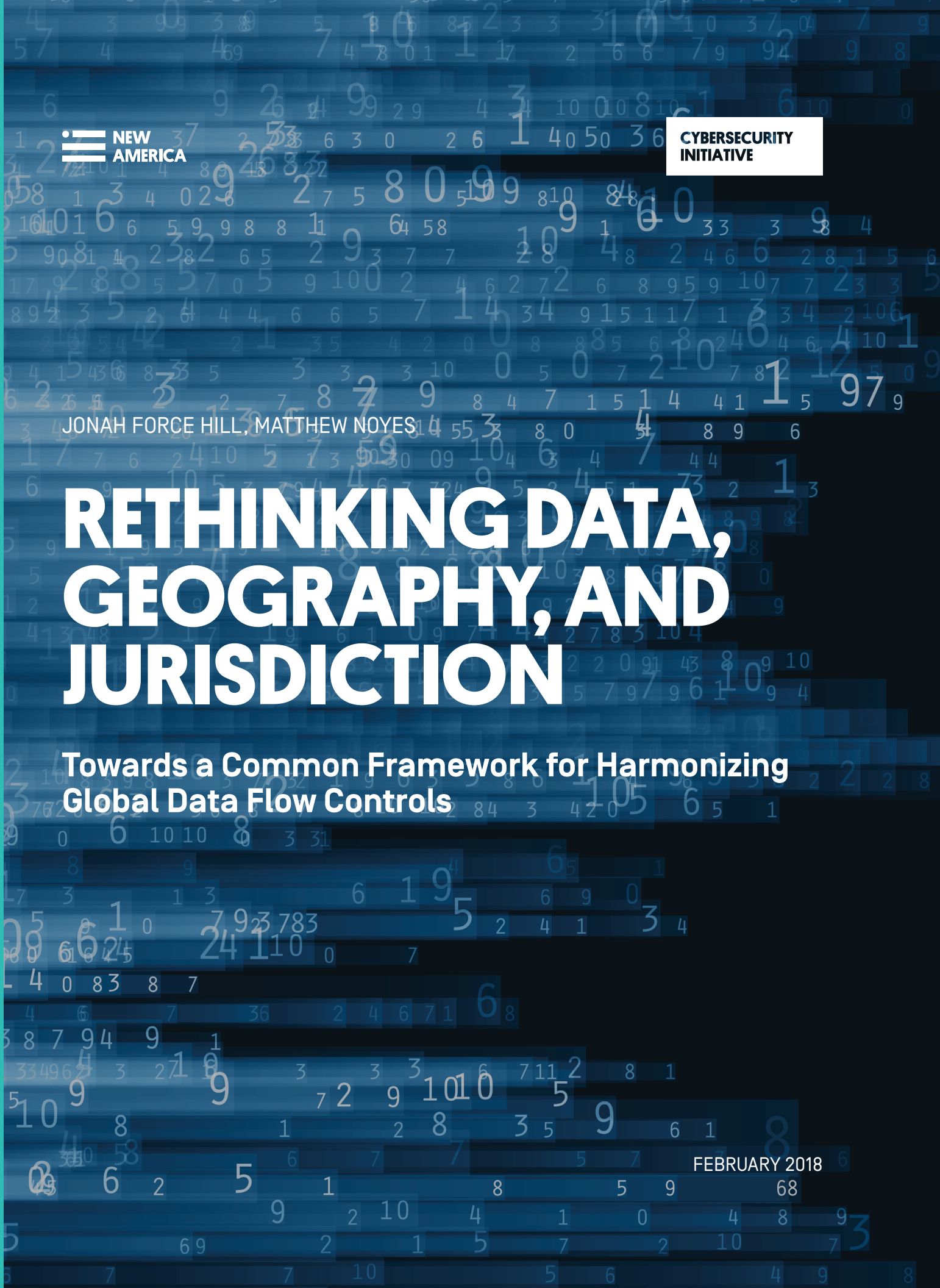


NEW AMERICA

CYBERSECURITY INITIATIVE

JONAH FORCE HILL, MATTHEW NOYES

RETHINKING DATA, GEOGRAPHY, AND JURISDICTION

Towards a Common Framework for Harmonizing Global Data Flow Controls

FEBRUARY 2018

About the Authors

Jonah Force Hill is an Internet Policy Specialist at the U.S. Department of Commerce and a Cybersecurity Fellow at New America.

Matthew Noyes is the Director of Cyber Policy and Strategy at the U.S. Secret Service and a Major in the U.S. Army Reserve assigned to the cyber policy office within the Office of the Secretary of Defense.

The authors studied together at Harvard's John F. Kennedy School of Government. They developed this paper through discussions in the Transatlantic Digital Debates, a joint-venture of New America and the Global Public Policy Institute, aimed at advancing transatlantic cooperation in the digital age, particularly between the United States and Germany. The views expressed here are their own and should not be interpreted as official U.S. government policy.

This paper will appear as a chapter in forthcoming edited volume, *Rewired: Cybersecurity Governance*, Dr. Ryan Ellis and Vivek Mohan (Eds), Wiley Publishing, 2018.

About New America

New America is committed to renewing American politics, prosperity, and purpose in the Digital Age. We generate big ideas, bridge the gap between technology and policy, and curate broad public conversation. We combine the best of a policy research institute, technology laboratory, public forum, media platform, and a venture capital fund for ideas. We are a distinctive community of thinkers, writers, researchers, technologists, and community activists who believe deeply in the possibility of American renewal.

Find out more at **newamerica.org/our-story**.

About the Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring New America's focus on big ideas, bringing together technology and policy, and public engagement to the cybersecurity conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. A collaboration between New America's Open Technology Institute and International Security program, our work explores important cybersecurity policy questions at all levels of government and policy making, from the state and local to national and international. Examining issues from the vulnerabilities equities process in governments and the importance of cybersecurity policy at the state and local level to the potential of strong and stable international regimes to promote better cybersecurity, New America's Cybersecurity Initiative seeks to address issues others can't or don't and create impact at scale.

Our work is made possible through the generous support of the Florida International University, the William and Flora Hewlett Foundation, Microsoft Corporation, the Government of the United Kingdom, Endgame Inc., and the MITRE Corporation.

Find out more: **newamerica.org/cybersecurity-initiative**

Contents

EXECUTIVE SUMMARY

The Internet, and the global free flow of data that it has enabled, has undercut long-standing legal, normative, and procedural arrangements governing the control of information. Across the globe, governments and multinational companies alike are discovering that the prevailing geography-centric approach to data and jurisdiction is simply incompatible with the world of globalized digital communications. They are finding that prior methods of controlling information—such as those used to protect privacy, enforce intellectual property rights, and provide law enforcement access to information for criminal cases—are increasingly being challenged by the hard reality that data today recognizes no national borders.

Through an analysis of the most notable legal, policy, and diplomatic challenges emerging out of the globalization of data—and the various responses to those challenges—this paper makes the case that the international community ought to reject geographic-based data control frameworks. Alternatively, it argues, nations should adopt jurisdictional and operational frameworks that are geography-agnostic and premised instead on data flow "control points," the levers of control over a particular information system. The paper offers a control point framework for digital policymaking, which the authors derive from *control point analysis* and the *contextual integrity model*, two analytic methodologies designed to allow for technical policy discussions in computer engineering and digital privacy law, respectively. Finally, it proffers some recommendations for how the international community might harmonize various national approaches to digital law and policy in a way that is consistent with a control point approach.

INTRODUCTION

The Internet and the spread of modern digital communications have fundamentally upended the rules, norms, and mechanisms governing the flow of information around the world. From the first moment in time when governments kept written records of taxes levied and paid, and merchants kept records of buyers and sellers of goods, the information contained in those records occupied a known physical place, for example, at the business, or in the counting house. If one wanted to review those records, the task was simple—go to the physical place where the records were kept. Records may have been hidden, but they would generally be found near where they were made or used.

Today, however, with the advent of the Internet (and other global digital networks), digitized information (hereafter, simply "data") is regularly stored by multinational companies on computers that are physically located far away from the places from which the data originated or is used. Data is often copied and then stored and/or cached in multiple servers in disparate locations in several countries simultaneously. And, through use of modern data storage methods, data is increasingly being sliced into small portions and then distributed out across the world, shifting from one geography to another (often on an automated basis), as more efficient storage space becomes available elsewhere on the globe.[1]

This sea-change in the way data moves, is stored, and is distributed around the world is challenging longstanding approaches to controlling information flows. The interrelated questions—who "owns" what data, which sovereign laws apply to which data overseas, and when and how governments should assist one another with law enforcement investigations seeking to obtain data—have quickly become some of the most vexing and persistent questions of law and policy in the Internet age. Governments, tech companies, and legal experts across the world are struggling to reconcile the Internet's globalization of data with the often-competing demands of privacy, national sovereignty, global trade, and the desire to maintain longstanding notions of international comity and cooperation.

What is emerging is a set of highly complex and intertwined international disputes that are threatening the growth of the Internet and the broader information economy, while simultaneously undermining international cooperation on other pressing global issues.[2] These are disputes that have become more frequent and more contentious over time; and the responses by governments have become increasingly assertive. Around the world, governments are advancing new legal and policy regimes seeking to address aspects of the problem, such as new privacy legislation. But many (if not most) of these regimes are premised on the

geographic location of data as the basis for asserting legal jurisdiction, which only serves to further exacerbate the underlying problem.[3] It is becoming clear that the current piecemeal response by the international community needs to be radically rethought.

In this paper, we describe these various challenges as a means of illustrating the need for a new and comprehensive approach to data flow controls,[4] an approach that can allow for the harmonization of the various national approaches in use today. As a first step, we propose a framework and ontology for mapping data flow controls which we derive from control points analysis (CPA)[5] and the contextual integrity model (CIM),[6] two established analytic methodologies designed to allow for technical policy discussions in computer engineering and digital privacy theory, respectively. Critically, we note, neither CPA nor CIM use geography as a primary factor in their analytic approaches. Finally, we offer some potential avenues for advancing international cooperation on several of the more troublesome international data flow conflicts, consistent with a control point framework.

When reading this paper, it is important not to interpret our advocacy and proposed framework as an endorsement of any new omnibus international legal instrument, such as a global treaty on cybercrime. On the contrary, given the complexity of the problems and the diverse set of interests and stakeholders involved, we suspect that any solution will require multiple arrangements—some legal, some normative, and some procedural. Nevertheless, we maintain that absent a harmonized approach to data flow controls, the escalating fragmentation of the Internet will further split the global Internet into separate, semi-sovereign networks.[7] This fragmentation, we argue, would fundamentally degrade the Internet's future potential for innovation, economic growth, and the other social, scientific, and democratic advancements we have come to expect from today's global network.[8] The status quo of conflicting data flow controls is no longer sustainable; a fundamentally different approach to data and jurisdiction is required.

Absent a harmonized approach to data flow controls, the escalating fragmentation of the Internet will further split the global Internet into separate, semi-sovereign networks.

THE CHALLENGE OF EXTRATERRITORIAL DATA

The Challenge to Law Enforcement

One of the core functions of any government is the enforcement of law, particularly criminal law.[9] However, this core function is challenged by modern transnational data flows and the resulting inability of governments to access or control the information necessary to effectively enforce their laws. In the pre-Internet era, there were comparatively few and limited circumstances in which law enforcement officials needed to exert their legal authorities overseas.[10] Police might have needed to track a murder suspect escaping to a neighboring country, or to investigate an organized crime group laundering money through an overseas bank. However, with the rise of globalized information flows and commercial data storage practices, information necessary to investigations and prosecutions is now located all over the world, generally under the control of private companies. Even routine investigations of an entirely domestic nature often today require law enforcement officials to seek out critical digital evidence stored beyond their borders.

The Problem With MLATs

Cross-border law enforcement information sharing has historically been provided through negotiated assistance amongst national governments, most importantly through the mutual legal assistance treaty (MLAT) system. MLATs are broadly worded bilateral (and occasionally multilateral) treaties that are designed to allow for cooperation on a specified range of law enforcement issues, such as locating and extraditing individuals, freezing assets, requesting searches and seizures, and taking testimony.[11]

In recent years, the MLAT system has struggled to keep pace with the growth of globalized data and the expansion of cloud-based services and data storage.[12] As data critical to domestic investigations has moved overseas, the total number of MLAT requests has skyrocketed. The United States Department of Justice (DOJ)—which both processes MLAT requests from other governments and issues MLAT requests for overseas assistance with its own investigations—estimated in 2014 that over the past decade, the "number of MLAT requests for assistance from foreign authorities has increased by nearly 60 percent, and the number of requests for computer records has increased ten-fold."[13]

Compounding the problem, the issues falling under MLAT provisions have grown vastly more complex in recent years, exceeding the scope of treaty

language. This is because most of today's MLATs were drafted prior to the Internet's widespread global adoption and therefore few of the treaties address core questions of data and jurisdiction, such as how to treat data held overseas by a subsidiary of a domestic parent company. Perhaps most significantly, MLATs frequently do not specify what constitutes "protected data" or under what conditions "content" differs from "metadata" for the purposes of information sharing.[14] This lack of clarity and agreement on terminology hinders cooperation between states with differing domestic legal regimes and understanding of these terms.

The increase in MLAT requests, and the accompanying legal uncertainty surrounding how and when privacy and data protection regulations apply in investigations, has caused significant delays in responding to requests for legal assistance. The President's Review Group on Intelligence and Communication Technologies (the independent review board tasked with assessing U.S. intelligence collection practices following Edward Snowden's disclosures) estimated in 2013 that it takes an average of ten months for the DOJ to process MLAT requests, and can take years.[15] Foreign countries' processing of MLAT requests are similarly drawn out, and can take far longer.[16]

> **Most of today's MLATs were drafted prior to the Internet's widespread global adoption and therefore few of the treaties address core questions of data and jurisdiction.**

Further adding to the MLAT backlog, various so-called "blocking features" in domestic privacy law often prohibit or constrain online hosts and providers from responding to requests for data from foreign authorities directly. These blocking features, such those as contained in the Electronic Communications Privacy Act (ECPA) in the United States,[17] are intended to provide privacy protections to domestic citizens by preventing companies operating domestically from being compelled to transfer data to foreign law enforcement without a preliminary domestic government review to ensure that the overseas request is valid.[18] But as more and more of the world's data is stored outside of national jurisdictions—most critically in the United States, where the blocking provisions of ECPA are in force—governments around the world are finding that legal provisions designed to protect privacy are forcing law enforcement agencies to operate exclusively through the MLAT system. This is significantly delaying, or even preventing, otherwise lawful government access to data critical to domestic criminal matters.

Expectedly, such delays are unacceptable to law enforcement officials who urgently need information for their cases. As former U.K. Independent Reviewer of Terrorism Legislation David Anderson QC summarized in his 2014 report,

"there is little dispute that the MLAT route is currently ineffective. Principally this is because it is too slow to meet the needs of an investigation, particularly in relation to a dynamic conspiracy; a request to the United States, for instance, might typically take nine months to produce what is sought."[19]

For example, the Brazilian government has been frustrated by extended delays in the MLAT system, especially pertaining to its request for information from Google's U.S.-based servers for several cases pending before the Brazilian Supreme Court.[20] India too has found the MLAT process with the United States to be ineffective. It has often invoked the U.S.-India MLAT to request that America serve summonses on Google, Facebook, Twitter, and others for failing to prevent the dissemination of online speech prohibited under Indian law. But these requests have been repeatedly rejected due to U.S. civil liberties requirements and privacy protections enshrined in ECPA.[21] The United Kingdom, France, China, and many others have faced similar obstacles to receiving data or enforcing domestic laws.

U.S. law enforcement has likewise found that the MLAT system can be an ineffective means of acquiring data stored overseas. This is despite the United States' unique position as the home of the lion's share of stored electronics communications data maintained by U.S.-headquartered technology companies. Rather than wait months for an MLAT request to be fulfilled, the United States has regularly relied upon court orders to compel providers to produce data directly, regardless of where that data might be stored. Yet, even with court orders in hand, U.S. law enforcement officials are experiencing challenges. Most famously, in the *Microsoft v. United States* case,[22] the DOJ is seeking data from a Microsoft Outlook account based in Ireland for a criminal investigation in the Southern District of New York. Prosecutors obtained a Stored Communications Act (SCA) warrant instructing Microsoft to produce information from the Ireland-based account directly. However, Microsoft challenged the warrant, based on the legal assertion that the SCA does not permit extraterritorial application to data stored outside of the United States.[23] This argument persuaded the Second Circuit panel when it heard the case, ruling that a warrant issued under Section 2703 of the Stored Communications Act could not compel American companies to produce data stored in servers outside the United States.[24] The U.S. government has subsequently sought review by the Supreme Court,[25] which on October 16, 2017 agreed to take up the case.[26]

However, one policy consideration was also central to Microsoft's position: the company argued that circumvention of the MLAT process sets a troubling precedent for future extraterritorial data requests. Meanwhile, the Irish government both noted that they would consider an MLAT request made by U.S. authorities, and that under Irish law their courts have the authority to compel the production of documents stored abroad, but should seek to avoid violating the law of a foreign sovereign. However, the Irish government was silent on the question of whether there would be a violation of their domestic laws if Microsoft were compelled to produce data stored in Ireland.[27]

The Microsoft case is hardly unique. Other cases touching on similar transnational data access challenges have gained widespread attention. These cases often involve exigent matters, which the MLAT process is particularly ill-suited to address in a timely matter. For example, in January 2017, a Mississippi investigator obtained a search warrant for an email account of a suspected criminal involved in exchanging and viewing images of child exploitation. As of June 2017, the contents of the account—which are stored outside of the United States—had not been provided to law enforcement.[28] In California, likewise, investigators have waited months to receive the contents of an overseas account pertaining to the disappearance and suspected murder of a young child.[29]

It is also worth noting here that MLATs and existing legal regimes have, at times, been ineffective not because they are slow or because their language fails to account for digitized information, but because the data required by law enforcement is not located in *any specific single geographic location*. This has been the situation in a number of prominent court cases involving Google, which as a regular practice stores data in a cloud architecture through a process called "sharding."[30] This is a process whereby data is split into small portions that are in turn spread out and stored in multiple servers, which are themselves often spread across several countries. In such a data storage architecture, it is impractical to identify what government has jurisdiction over the information when using a geographic basis for such issues. As of September 2017, at least eleven magistrate and district judges, outside of the Second Circuit, have ruled that Google is required to reassemble the needed data and turn it over to law enforcement in the United States, irrespective of where those pieces of information are located.[31]

These Google rulings do little to resolve the underlying international policy questions surrounding jurisdiction over data, nor do they resolve the underlying questions contained in the Microsoft-Ireland case. However, they do represent a pragmatic recognition by the U.S. courts that

the geographic location of data should not be a predominant question. The cases were decided, consistent with U.S. law governing subpoenas, on the grounds that the entity (here, Google) was lawfully subject to the government's subpoena process, and had it in its power to produce the information. The courts did not focus on the location of the stored data as the particularly relevant factor.[32] Yet while this pragmatic interpretation may be advantageous to prosecutors and regulators in the United States, it provides no assistance to their foreign counterparts whose governments have no such robust authority over Google and the other American Internet giants.

Alternative Approaches to MLATs

It is clear that the MLAT system has, in many ways, failed to address the challenges of transnational law enforcement cooperation in the modern Internet era.[33] Reform of the MLAT system (i.e., efforts to modernize the mechanisms by which data requests are processed, to increase funding to speed up processing of MLAT requests, or to renegotiate the treaties to take into account modern digitized evidentiary requirements) has become the elementary fix and the topic *du jour* of academics and justice ministries around the world looking to address this problem.[34]

But while discussions of MLAT reform have proliferated and have raised a number of potentially fruitful improvements to the existing system,[35] the reality is that little substantive progress has been made to date. MLAT modernization efforts have been lethargic. In fact, the problem seems only to be getting worse, as governments are finding that today's MLAT system simply does not allow—and indeed may not be structurally designed to allow—for the kind of rapid international cooperation that is required in today's globalized digital environment.

As a result of glacial progress on MLAT reform, and in recognition of the increasing demand for transnational access to evidence, governments are now looking for alternative approaches, or bypasses, to MLATs as a means of acquiring the data they need. One seemingly straightforward solution has been to simply enable expanded reach into overseas jurisdictions for domestic law enforcement authorities. For instance, lawmakers in the United States have been exploring whether or not to amend the Stored Communications Act (SCA) to clarify that court orders, issued pursuant the act, can compel the production of data stored outside of the United States; thus, by statute, effectively overturning the Second Circuit's ruling in Microsoft-Ireland.[36]

Some governments are expanding their police power in a more problematic direction, however, by seeking to provide their law enforcement agencies with authority to forcefully infiltrate (i.e. to hack) the computer systems of companies overseas. State-authorized hacking allows law enforcement agencies to directly access the data without going through an MLAT, and without obtaining the cooperation of the private company with access to the data.[37] Troublingly, these authorities are often granted with little regard for the laws of other countries or the privacy and property rights of foreign companies and individuals.

Of the countries pursuing this approach, China appears to be acting most conspicuously and aggressively. There, regulations issued in 2016 by the Supreme People's Court, the Supreme People's Procuratorate (China's prosecutor), and the Public Security Bureau, appear to authorize "the unilateral extraction of data concerning anyone (or any company) being investigated under Chinese criminal law from servers and hard drives located outside of China."[38] Others describe this regulation as merely restating what has been longstanding Chinese law enforcement practice.[39] Either way, the 2016 regulation makes it clear that Chinese law enforcement agencies are permitted, under Chinese law, to remotely access any computer system anywhere in the world.[40]

But the Chinese are not alone. In the United States, recent revisions to Rule 41 of the Federal Rules of Criminal Procedure has clarified that magistrate

judges have the jurisdiction to issue search warrants authorizing law enforcement to "lawfully hack" computer systems that are in unknown locations—an authority that may lead to U.S. authorities unwittingly searching computers located overseas. Specifically, under Rule 41 magistrate judges have the power to issue search warrants to U.S. law enforcement in situations in which the location of the computer "has been concealed through technological means," or in the case of a botnet where computers "have been damaged without authorization and are located in five or more districts."[41]

More promising efforts have focused on creating new diplomatic arrangements separate from, but complementary to, MLATs, which would allow law enforcement agencies to directly request data from overseas firms in the participating countries.

It can be argued that these readings of these Chinese and American approaches (or at least authorities) are vastly divergent in their scope, with the U.S. powers much more narrowly tailored and, of course, subject to review of judicial officers not subservient to law enforcement or political interests. But as many prominent computer security experts have noted, the "lawful hacking" approach (which has been discussed in other settings at length, often in the context of the "going dark" debate)[42] risks further undermining global cybersecurity by adding law enforcement agencies to the already crowded cadre of militaries,[43] intelligence agencies, and cyber-criminals that are routinely hacking overseas computer systems and stockpiling software vulnerabilities and offensive exploits, rather than working with technology providers to correct those vulnerabilities.[44]

Some observers have proposed a hybrid model that considers a number of factors to determine what process the governments should use to obtain data. For example, a July 2017 paper published by the Information Technology & Innovation Foundation (ITIF) proposed a model that focuses first on the location of the stored data, with the location of the business itself a secondary factor.[45] However, such a model fails to consider where a crime occurred, the nature of the offense, or situations where a business intentionally obscures its location. And, like the other alternatives to MLATs, the approach seems to reinforce the longstanding notion that the geographic location where data is stored is a particularly relevant consideration, ignoring the reality that the geographic location of data is often unknown.[46]

More promising efforts have focused on creating new diplomatic arrangements separate from, but complementary to, MLATs, which would allow law enforcement agencies to directly request data from overseas firms in the participating countries.[47] Most notably, the U.S. and U.K. governments have been exploring a new diplomatic and legal instrument, the *U.K.-U.S. Bilateral Agreement on Data Access*,[48] as a potential path forward. If accepted by both nations, the agreement would provide law enforcement agencies in the two countries with an effective alternative to the MLAT system (under certain specified conditions and subject to new oversight mechanisms) and make requests for data to the providers holding the data directly. Adoption of the proposed agreement would require that the United States amend ECPA to allow American companies to fulfill U.K. requests for data without violating ECPA's "blocking features" that now prevent American companies from complying with foreign law enforcement requests that have not gone through the U.S. justice system.[49] Negotiators on both sides of the Atlantic are hoping to extend this system to additional countries as well, but it is currently unclear how this kind of arrangement might expand beyond the United States and United Kingdom to countries with less similar or less well-developed legal systems with fewer comparable oversight mechanisms.[50]

The Challenge to Regulators

While law enforcement's inability to access data stored overseas may be the primary driver of the debate surrounding data jurisdiction, there are other unresolved questions of extraterritoriality that are presenting similar challenges and placing additional pressure on existing systems of international cooperation. These span sectors, from financial regulatory issues to divergent notions of intellectual property protection. But perhaps most importantly, the regulation of online speech, content, and privacy have emerged as the some of the most contentious and impactful in matters of public policy and international cooperation.

Content and Speech

From the earliest days of the Internet and the digitization of global media, governments have been encountering significant difficulties in curtailing the production and distribution of illegal, illicit, and/or harmful content online. However, as an increasing percentage of the world's content becomes digitized and made available globally, thus allowing Internet users in one country to view or host content that may be illegal in another, the challenges surrounding the control of content and speech have greatly proliferated and intensified.

This is primarily due to the fact that the rules covering the control and access to information vary widely from country to country. In the United States, for instance, while the First Amendment protects most forms of speech, there are still forms of information and content, such as child pornography or defamatory speech, which are prohibited or actionable under U.S. law. For democracies without American-style First Amendment protections, the range of restricted speech and content is generally broader and more fluid. Domestic laws and regulations in these countries may prohibit such content as hate speech or radicalizing propaganda (categories of speech generally protected in the United States). Limitations are often even more expansive in non-democratic countries or in countries with strict religious laws, where broad categories of content that challenge the state or insult religious figures or symbols are strictly prohibited. In all these countries, democratic or otherwise, there are specific intellectual property rules which limit what movies, music, and other protected material Internet users may access. These rules are often rendered toothless when the proscribed material is hosted overseas.

> **Companies are caught in the middle of intersecting legal systems and contradictory demands from regulators, constantly being forced to decide between two sets of government rules or to weigh the legal merits or human rights implications of a particular request.**

These disparate national approaches to speech and content are challenging anachronistic notions of national sovereignty based primarily on geography. Regulators are often unable to force providers and hosts to take down content that is prohibited under their nation's domestic laws. Companies are caught in the middle of intersecting legal systems and contradictory demands from regulators, constantly being forced to decide between two sets of government rules or to weigh the legal merits or human rights implications of a particular request.[51] Often, providers are unable to remove content in response to the demands of one country without potentially violating the laws of another. They are frequently left with no option but to take no action at all.

The recent Canadian case of *Google v. Equustek* provides an instructive example of how the enforcement of domestic content rules can have significant extraterritorial impacts. The case stems from a dispute between Equustek, a Canadian company, and Datalink, an American company,

over Datalink's allegedly unlawful acquisition of Equustek's confidential information and trade secrets and subsequent sale of counterfeit Equustek products. Equustek obtained an injunction from a British Columbia court that ordered Google (which, while not a party to the underlying litigation, provided search results linking to Datalink websites) to remove the infringing websites from its search index. This was an order to remove links to the infringing websites not just for searches initiated by persons located in Canada, but by all searchers across the globe. Google challenged the court order, but its appeal was ultimately denied by the Court of Appeal for British Columbia, a ruling which was then upheld by the Canadian Supreme Court.[52] Google has subsequently filed a complaint in the Northern District of California challenging the enforceability of the Canadian ruling,[53] arguing, among other things, that enforcement in the United States would violate the First Amendment.[54]

Google and others have noted the potentially calamitous precedent the Equustek cases present.[55] As Andrew Woods notes, "[t]he parties [did] not dispute Canada's authority to settle the underlying lawsuit between Equustek and Datalink, nor do they dispute Canada's authority to enjoin Google from displaying content that violates Canadian law. Rather, the parties dispute the *territorial reach* of that authority" (emphasis added).[56] By requiring Google to delist Datalink websites worldwide, the Canadian Equustek ruling has set a precedent that, if adopted in other jurisdictions, could result in forcing Internet intermediaries like Google to remove any offending material globally at the order of any court in any country. As Daphne Keller writes, "[t]he [Equustek case] was closely watched in part because of the message that it sends to other courts and governments, which are increasingly asserting their own appetites for global enforcement of national laws."[57]

The issues raised by court rulings that purport to have a global reach are similar to those seen in the so-called "right to be forgotten" debate, which concern the question of whether Internet users have a right to "de-index" certain information about themselves from Internet search results. This debate traces its roots back to 2013, when the European Court of Justice ruled[58] that European Council Directive 95/46 (the 1995 Data Protection Directive)[59] gives Europeans who feel they are being "misrepresented by search results that are no longer accurate or relevant" (for instance, information about crimes committed as a minor) the authority to "force search engines, like Google or Bing, to 'de-index' that information from their search results."[60] The information remain online at the original website, "but would no longer come up under certain search engine queries."[61]

De-indexing in this context presents search engines with a significant challenge, one similarly raised in the Equustek case: Can a search engine remove or de-index a particular web page in one country without deleting that information globally? In response to this challenge, Google and others have tried to limit de-indexing measures to those searches made within the jurisdiction of a particular request through the use of geolocation techniques and by only de-indexing searches made within specific country-code top-level domains,[62] such as www.google.de for de-indexing requests made in Germany, for example. According to Google, regulators (in Europe, in particular) have found this limited approach unacceptable,[63] noting that Internet users can easily circumvent these measures by visiting www.google.com, and thus have insisted that results be removed on a global scale. In light of the push by countries in Latin America,[64] Asia,[65] and elsewhere for their own de-indexing requirements, the growth of the "right to be forgotten" trend seems likely to continue, and the conflicts surrounding the extraterritorial application of domestic law and incompatibility of national approach likely to intensify.

Privacy and Data Protection

We are witnessing a similar conflict between divergent national approaches with respect to online privacy. Lawmakers around the world have been working to modernize national privacy

and personal data protection rules to keep pace with developments in the collection, control, and sharing of personal information. Often contained within these modernization efforts are regulatory provisions that, as a prerequisite for the cross-border transfer of personal information to another country, require a third country receiving personal data to have its domestic privacy protections deemed "adequate."[66] This has been the approach taken by the European Union,[67] most notably, but it is also being adopted as a generalized model in other large markets, such as Brazil.[68] China[69] and Russia[70] have imposed even more onerous requirements on personal data transfers.

Yet, while these kinds of arrangements might be well-intentioned efforts to protect personal data (whether or not such policies are actually disguised attempts at trade protectionism, or a backhanded effort to enable law enforcement access to data, is another important question beyond the scope of this paper) the incompatibility of the various national approaches runs the risk of fracturing the Internet by preventing data flows to countries with perceived "inadequate" data protection rules or oversight. Indeed, when in 2015 the European Court of Justice invalidated the longstanding *E.U.-U.S. Safe Harbor Agreement*,[71] which had previously provided a core legal mechanism for European personal data to travel to the United States, this risk of a catastrophic fissure in the Internet nearly became a reality.[72]

THE THREAT OF DATA LOCALIZATION

In response to these various, interrelated challenges—law enforcement access to evidence, conflicts over intellectual property protection, content regulation, online privacy, etc.—a number of governments have implemented, are implementing, or are considering implementing, so-called "data localization" requirements. These are rules that seek to limit the storage, movement, and/or processing of data to specific geographies and jurisdictions, or that limit the companies that are legally permitted to manage data based upon the company's nation of incorporation or principal situs of operations and management. To date, more than 20 countries have implemented or are considering implementing such restrictions.[73]

One of this paper's authors wrote a lengthy piece on the motivations behind the data localization movement and the many reasons why it is deeply problematical.[74] But in short, through data localization measures, governments are seeking to address their difficulties in obtaining what they

believe is appropriate relief in foreign jurisdictions (principally in the United States), as well as the inability of their law enforcement and regulatory agencies to control data or access the data they want in one fell swoop. But once again, while efforts to put in place such measures might in many cases be well-meaning (although, it must also be noted that there is a protectionist incentive at play here as well, with some governments offering security and privacy concerns as a pretext for erecting trade barriers through these policies), data localization rules are problematic on a number of fronts. By restricting data flows and competition between firms, data localization policies raise costs for Internet users and businesses and reduce technological innovation. In countries with underdeveloped oversight mechanisms, they may enable domestic surveillance and abuses of power. And perhaps most worryingly, data localization policies, if implemented on a wide international scale, risk profoundly fragmenting the Internet, turning back the clock on the integration of global communication and commerce, and putting into jeopardy the myriad of societal benefits that a globally integrated Internet has engendered.

Moreover, data localization policies actually do little to improve security or to protect privacy. The global nature of Internet communications has made data security or privacy almost entirely independent of location. Data breaches can and do occur anywhere and privacy violations happen in every country. Security and privacy are primarily functions of the quality and effectiveness of the mechanisms and controls maintained to protect the data in question, not where the data physically resides. What matters is not *where* data is stored, but *how* it is stored. Even with respect to law enforcement access, data localization policies are generally not an effective means of providing access to data, as recent criminal cases involving encryption have demonstrated.[75]

Ultimately, data localization policies should be viewed as an understandable—however deeply flawed and problematic—reaction by governments unable to cope with the diverse set of challenges presented by the globalization of data described above (as well as others that were not discussed).[76] But data localization policies are not a viable solution to the range of problems governments are facing and are likely to do far more harm than good. They present a host of unintended consequences and only serve to further institutionalize, and thus perpetuate, outdated notions of geography and jurisdiction that do not comport with the realities of data in the twenty-first century.[77] An alternative to data localization, such as restrictions on data transfers predicated the notional protection of privacy, is desperately needed.

Data localization policies, if implemented on a wide international scale, risk profoundly fragmenting the Internet, turning back the clock on the integration of global communication and commerce, and putting into jeopardy the myriad of societal benefits that a globally integrated Internet has engendered.

A NEW APPROACH TO DATA FLOW CONTROLS

The diversity and complexity of the legal and policy challenges described above, and the requisite international policy coordination required to address these challenges, are unquestionably daunting. It has become clear that an entirely new framework for thinking about data and jurisdiction is needed, as well a renewed global effort to harmonize the rules, norms, and mechanisms of international cooperation.

Considering the inherent contradictions of geography-based controls[78] described above, we propose a common framework for data flow controls that uses a limited set of relevant *premises for data flow controls* that are applied based on a state's relationship with certain *control points,* rather than the physical location of data. This proposed policy framework does not itself harmonize data flow controls among nations, rather, it provides policymakers with a common lexicon and ontology to discuss and formulate agreed-upon standards. It is a framework that could be leveraged as the basis for new or expanded international agreements, regulations, and/or statutes, and even could help facilitate the automation of data flow processes, such as MLAT requests.

Control Points Analysis

National governments have consistently demonstrated that they have robust means of exerting sovereign control over communications, irrespective of the location of that data.[79] This sovereign control is exerted through control points, the levers of control over a particular information system.[80] These include such entities as telecommunications providers, search engines, Internet service providers, hosting companies, and payment service providers, as well as technical infrastructure over which those entities have control. Control point analysis (CPA), as described by MIT's David Clark, is a methodology for identifying the elements of an Internet system and the entities with power and control over those various elements.[81]

Thus, CPA provides a practical methodology for identifying the full set of entities involved in a data flow on the Internet and helps identify options for impacting that data flow. By focusing on the full set of control points, rather than on the physical location of data storage or hosting, governments can identify opportunities to exert appropriate sovereign influence within a broader system. They can do this through the actors that have control of key components mechanisms of a

data flow, independent of the geographic location of the data in question. Accordingly, any effort to establish a data flow control should begin with an analysis of the available control points as a means of identifying the full range of actors and options capable of achieving the desired effect. Based upon that analysis, policymakers can determine the most appropriate action in a particular circumstance. In this approach, geography is no longer the primary analytical consideration.

With all that said, adopting a non-geographic jurisdiction model based upon CPA in no way renders geography irrelevant to policy considerations. The physical location of companies, where their employees live and work, and where infrastructure and customers are physically located, all remain critical factors and determine the control points.

> **Any effort to establish a data flow control should begin with an analysis of the available control points as a means of identifying the full range of actors and options capable of achieving the desired effect.**

Moreover, CPA does not resolve the critical normative and policy question of the appropriate legal obligations to impose on the various control points. Rather, it provides policymakers the full range of options by focusing on their relationship with, and influence over, the various control points. Policymakers must still identify which control points are the most appropriate to leverage, how and when to restrict actions taken towards actors which maintain influence over specific control points, and what enforcement and appeal mechanisms should be available for achieving the desired impact. Throughout this entire process—from control point identification to selected government action—it is necessary to ensure that such determinations are grounded in sound legal, ethical, and normative principles, rather than a nationalist or populist political considerations. Here, leveraging processes that involve a diverse collection of stakeholders can help to ensure a more fulsome consideration of the merits of a particular control.

As an example of this process in action and the kinds of constraints governments need to weigh, consider the challenge of the "right to be forgotten" highlighted above. In addition to identifying which controls points are available to enforce de-indexing orders, governments need to decide whether the search engines (which have the ability to de-index certain search results), the platforms (that supply the data), the domain registrars (that host the data), or the ISPs (that serve the data to a particular audience), are the most appropriate control point over which to exert influence. In certain cases, perhaps all four control points—search engines, platforms, domain hosts, and ISPs—should be leveraged in tandem. Again, CPA alone does not help government actors determine which actions should be taken against which control point or points. Rather, it aids in identifying the full set of control points and associated entities involved in the data flow, thus enabling policymakers to identify the most appropriate control point and action for achieving a particular effect.

A Common Framework for Data Flow Controls

In order to help governments decide when and how to utilize the control points available to them, we suggest employing a policy framework derived and abstracted from Helen Nissenbaum's popular contextual integrity model (CIM).[82] CIM provides a common set of factors for determining privacy-appropriate data flow controls based upon both the normative and the legal privacy standards of a particular "context," such as healthcare or finance. It "ties adequate protection for privacy to norms of [those specific contexts], demanding that information gathering and dissemination be appropriate to that context and obey the governing

norms of distribution within it."[83] Like CPA, it does not include a reference to the location of the information.

Nissenbaum describes the fundamentals of CIM norms based upon five independent parameters or criteria. These five factors help policymakers identify, based upon contextual information norms, whether or not data flows or data flow controls are appropriate from a privacy perspective. They include:

- The **data subject** (such as a hospital patient, a customer, or a viewer of a movie)
- The **sender of the data** (such as a bank, the police, an online retailer, or a friend)
- The **recipient of the data** (such as a bank, the police, an online retailer, or a friend)
- The **information type** (such as email contents, metadata, or social security numbers)
- The **transmission principle** (such as consent, coercion, theft, or sale)

While the CIM was designed specifically to address privacy of digital communications, by generalizing Nissenbaum's model, we seek to address the full range of data flow issues through a single ontology. Our aim here is that this ontology is interoperable and consistent with the existing CIM framework (which is already widely used and recognized by privacy practitioners and theorists).

Accordingly, we propose our own three-factor model for instituting data flow controls, which is premised on: **[1] an entity's role in the data flow**, **[2] the nature of the data**, and **[3] the ownership, access, or other rights to the data**.

[1] An Entity's Role in the Data Flow[84]

An entity's role in the data flow includes not just the sender and recipient, but also the creator, transmitter, storage provider, transporter, software system provider, platform owner, and domain name registry, among others. Essentially, this factor encompasses any entity which may be identified through CPA that has a role, and therefore ability, to directly affect the data flow from creation to reception, rather than simply the sender and recipient specified in the CIM. States have a variety of means to exert sovereign control or influence upon such entities, often independent of their physical location, and often seek the assistance of foreign states to do so.

[2] The Nature of the Data[85]

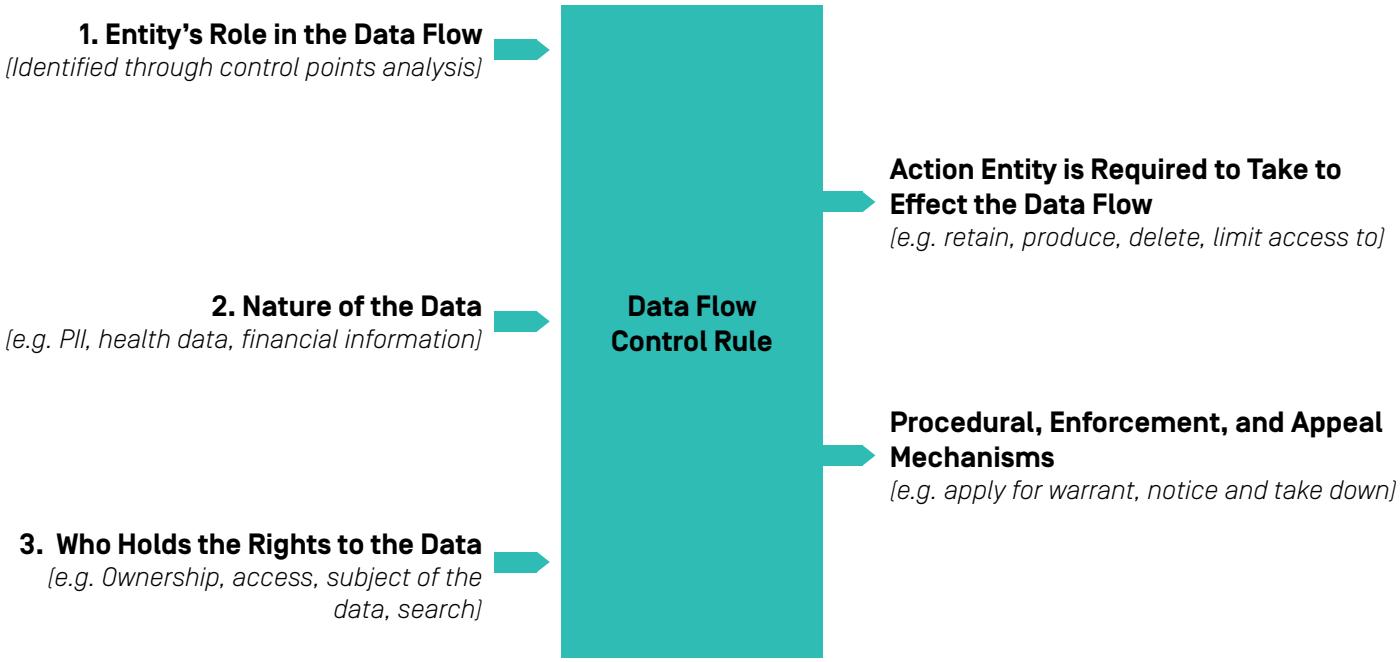
The nature of the data refers to a wide variety of specified categories of data. For example, this could be health information of a patient, sensitive personally identifiable information, hate speech, child pornography, or evidence of a crime. Data may fit within multiple categories, and nations will certainly disagree over how to scope the categories of data and the associated controls they should leverage over such categories.

[3] Ownership, Access, or Other Rights to the Data[86]

Ownership or access rights to the data refers to who has lawful authority or right to the data. For example, the copyright holder possesses certain rights to the data, law enforcement authorities have legal authority to access to data in particular circumstances, and the person who is the subject of the data may have some rights related to the data flow.

These three factors could serve as the legal or policy basis by which a government authority could compel an entity involved in the data flow process to take a particular action. For example, a government may require a bank to: (1) preserve information about a customer's account, (2) keep records of who created or sent particular funds relevant to that account, (3) provide account data to a third party (for example, a law enforcement agency), (4) implement particular security protections to safeguard that account data, or (5)

Figure 1 | Three-Factor Model for Data Flow Controls



ensure the integrity of the data in question. All such requirements are applied to an entity involved in the data flow (the bank) to a specific nature of data (account records), and based upon their rights to the data (information in the bank's possession). The geographic location of the entities being compelled still matters, but the location of the data itself is irrelevant.

Again, this policy framework does not itself harmonize data flow controls across nations. Rather, it provides policymakers with a common vocabulary and ontology to discuss and formulate agreed-upon standards for specific control points and actions and could allow for the development of systems for automated requests. The legal and normative particulars of the various types of controls (for instance, requirements that a request go through independent judicial review or receive the consent of the owner or subject of the data) will, in each country, generally be based upon the laws and norms of its particular legal system. Nations are certain to maintain differences on the categories of data and actors upon which they impose these controls, the entities upon which they exert those controls, and the types of controls that they implement. These differences present their own risks. Less democratic countries will likely maintain a far more flexible interpretation of governmental powers than those countries in which the rule of law is robust. There will be opportunities for authoritarian governments to abuse a control point framework, such as we have described, towards undemocratic ends. Nevertheless, it is not clear that a control point framework would be any *worse* in that respect than the existing geographic-based system, and it could potentially could be significantly better. After all, the process of harmonization would necessarily embed less democratic countries into global diplomatic arrangements that would promote and reward domestic reforms. In any case, it is difficult to imagine that working towards harmonization, based upon our three factor model, would not substantially improve the effectiveness of today's deeply flawed efforts at controlling data flows.

RECOMMENDATIONS

Fostering a harmonized international system that supports appropriate transnational data flows under a common framework will require engagement on numerous contentious issues, including international law enforcement cooperation, online privacy, intellectual property, and even cybersecurity. Many, if not most, of these negotiations will need input and buy-in from lawmakers, various government ministries, industry, and civil society stakeholders. We recognize that there is unlikely to be broad international consensus on the key normative obligations and constraints that determine the appropriateness of data flows, or the suitable set of state controls to enforce new normative or legal agreements. Nevertheless, progress can be made by taking incremental steps and by using the framework we have described as a basis for additional harmonization efforts.

Recommendation #1: Establish a common framework for data flow controls through the development of international standards, norms, and principles.

As a first step towards harmonization, states will need to arrive at a baseline agreement on *terminology*, *norms*, and the *scope* of data flow policy issues, including for both control points and the policy considerations that determine the appropriateness of particular government actions. One potentially useful example of such a baseline agreement is the Asia-Pacific Economic Cooperation (APEC) Privacy Framework,[87] which has been used by the APEC member economies since 2004 to fashion comprehensive privacy legislation, and by industry groups and individual companies to implement self-regulatory standards.[88]

The privacy framework comprises a set of nine guiding principles and accompanying guidance on implementation to assist APEC Economies in developing consistent domestic approaches to personal information privacy protections. Unlike the EU Data Protection Directive, referenced above, the privacy framework is not binding and explicitly notes that APEC member economies will vary their implementation of the principles contained in the framework based upon "differences in [their] social, cultural, economic, and legal backgrounds."[89] By providing this kind of flexibility, the privacy framework seeks to reconcile digital privacy with business and societal needs, and at the same time, accords due recognition to cultural, legal, and other diversities that exist among member economies. The privacy framework was modelled upon the OECD *Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data* ("OECD Guidelines"), which at that time

represented the most widely-shared international consensus on "what constitutes fair and trustworthy treatment of personal information,"[90] and has since been updated to take into account of additional business and consumer input.

A similar approach to the privacy framework could be developed to address other thorny jurisdictional issues, such as cross-border law enforcement cooperation, using a CPA-type methodology. Government officials, companies, and civil society groups could come together and create a list of principles, implementation guidelines, and enforcement and arbitration mechanisms to govern law enforcement requests for data outside of the MLAT context, for instance, or for best practices for hate speech and intellectual property violations. The United Nations Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security (UNGGE), which has since 2004 has sought to develop international norms for responsible State behavior for offensive cyber activities, could also provide some lessons for how to, or how not to as the case may be, reach broad international agreement on baseline standards for cyberspace issues.[91]

> **"Law enforcement requests for digital evidence should be based on the location and nationality of users, not the location of data."**

Some of the largest Internet companies have already endorsed and indeed have sought to substantively advance this kind of standards-based approach to data flow controls.[92] For instance, Google, focusing specifically on the question of law enforcement's extraterritorial access to data, has proposed that "countries that honor baseline principles of privacy, human rights, and due process should be able to make direct requests to service providers for user data that pertains to serious crimes that happen within their borders and users who are within their jurisdiction." They go on to recommend that "United States and foreign governments…sign new agreements that could provide an alternative to the MLAT process," based upon adherence to those principles, and identify categories of standards for the U.S. government to promote, pertaining to such criteria as notice, redress, and reciprocity. Most importantly, they note "[l]aw enforcement requests for digital evidence should be based on the location and nationality of users, *not the location of data*" (emphasis added).[93]

In its proposal, Google does not attempt to offer its own set of standards. It instead relies upon those standards identified by the U.S. Department of Justice in its effort to develop the U.K.-U.S. data access agreement. Yet, while DOJ's set of baseline standards might serve as a starting point for further discussions, a far broader range of stakeholders beyond government officials ought to be included in the discussion and decision-making process for a standard or group of standards to be viewed as broadly legitimate. Such stakeholders should consider how the U.K.-U.S. data access agreement could be modified to accommodate participation from a broader set of countries.

Encouragingly, a number of groups are already taking on this task. One in particular, the Internet and Jurisdiction Policy Network (I&J),[94] based in Paris, has been seeking to bring in such a broader coalition. Since 2012, the I&J has been convening multi-stakeholder dialogues to advance collaboration on a number of the jurisdictional challenges highlighted above[95] and has established three working groups (one addressing questions of *data and jurisdiction*, one focused on *content and jurisdiction*, and another on *Internet domains and jurisdiction*) to develop standards for user notification, authentication of requesters, and the establishment of single points of contact for various data flow issues. Notably, among the preliminary policy recommendations of the process is an acknowledgement of "the strong benefit in moving away from [geographic-based] criteria and replacing it by the notion of control."[96] The work of the I&J is still in its early stages, but the initiative

and others like it have the potential to help facilitate the kind of baseline agreement needed to harmonize national approaches.

Recommendation #2: Formalize agreed-upon standards, norms, and principles through the adoption of voluntary and treaty-based international agreements.

Reaching agreement on standards and principles based upon a common framework, such as the one we have proposed, is just one piece of the harmonization puzzle. Those agreed-upon standards and principles must in turn be inserted into domestic law and policy and formalized through international agreements of various kinds. Implementation can take place in a number of venues, both internationally and domestically, and can be carried out through voluntary and binding agreements between states.

Here again the APEC Privacy Framework provides an instructive example of a voluntary, principles-based approach. Since 2011, the privacy framework has served as not just a baseline agreement on principles and guidelines for data privacy, as described above, but also as the basis for the APEC Cross Border Privacy Rules (CBPR) arrangement,[97] a voluntary, accountability-based system designed to facilitate privacy-respecting data flows among APEC economies. The CBPR system creates baseline standards that companies and governments can follow and reference, as well as mechanisms for enforcement and dispute resolution. It has allowed for interoperability on personal data protection regulations across vastly different national environments.

Under the CBPR system, companies and organizations that have a presence in the member countries, and that have adopted the system and chosen to implement privacy policies and practices consistent with the APEC Privacy Framework, gain certain regulatory protections when transferring certain private information to and from member countries. Once an organization has been certified for participation in the CBPR System by an APEC-recognized "Accountability Agent," these privacy policies and practices become legally binding domestically and enforceable by a domestic government authority to ensure compliance. For instance, in the case of the United States, the Federal Trade Commission (FTC) can levy penalties against companies for failing to meet their CBPR obligations. We believe similar voluntary, yet domestically enforceable, arrangements could be developed in other areas as well and in such venues as the G7 and G20 forums.

In certain cases, even more formalized approaches to harmonization may be necessary. For instance, international trade agreements such as the Trans-Pacific Partnership (TPP) (from which the United States has now withdrawn from negotiations),[98] the proposed Transatlantic Trade and Investment Partnership (T-TIP), or the Trade in Services Agreement (TiSA) might provide constructive avenues to cement standards and principles based on a common frame for data flow controls into law.[99] A number of these agreements already contain draft language addressing questions of data localization. But trade agreements could also serve as a vehicle by which countries can reach agreement on broader issues of data flow governance. By linking data flow questions to matters of trade, harmonization could substantially improve the global digital economy, similar to the impact on international business provided by the 1958 "Convention on the Recognition and Enforcement of Foreign Arbitral Awards" (also known as the "New York Convention"), which provides common legislative standards for the recognition of arbitration agreements, court recognition, and enforcement of foreign and non-domestic arbitral awards.[100] However, trade negotiations often take decades to complete,[101] if they are completed at all, and generally do not include non-governmental participants in the process of negotiations. Thus, they may not be the most appropriate means of reaching agreements on quickly moving and geopolitically complex digital issues.

Recommendation #3: Reform domestic law and policy frameworks consistent with agreed-upon standards, norms, and principles.

To ensure that new data control agreements and mechanisms are consistent with a common framework, a wide range of domestic laws will also need to be re-examined. For example, in the United States, ECPA will likely need to be amended to remove or reduce the general prohibition on U.S. companies responding to requests from foreign law enforcement (its "blocking features"). In addition, the scope of the Stored Communications Act, one of ECPA's three titles, needs to be clarified to ensure that law enforcement has the means to compel providers to produce data regardless of where the data is stored. The Department of Justice's May 24, 2017 proposal for "Secure and Privacy-Protective Access to Cross-border Electronic Data for Law Enforcement to Combat Serious Crime Including Terrorism," is an example of such a clarification. The proposal suggests measures to simultaneously reduce an existing geographic-based data flow control, while creating a structure that can be used to incentivize similar actions by foreign partners.[102] The major aspects of the proposal have received broad and strong support from Microsoft[103] and Google,[104] and should be seriously considered.[105]

Of course, the United States is not the only country with blocking provisions preventing foreign law enforcement officials from access to broad categories of data absent an MLAT request. A recent survey of the European Commission revealed that the majority of European member states' laws "do not cover/allow that service providers established in a Member State respond to direct requests from law enforcement authorities from another EU Member State or third country."[106] In fact, it appears that "only two Member States" allow for such cooperation. The United States could use its own privacy law update process to coax European governments to follow suit. This could happen by passing some form of federal legislation that would purport to address both baseline protections for privacy, sufficient to mollify other countries who perceive inadequacy, while simultaneously establishing a workable framework for access to data under legitimate circumstance. Irrespective of the specific laws in question, as domestic rules are reformed, governments should look for opportunities to leverage the reform process to incentivize other states to take similar and reciprocal actions.

Recommendation #4: Focus first on specific policy matters of broad international consensus, then move on to the more contentious issues.

An issue-specific approach could also provide significant opportunities for incremental progress and examples that can spread laterally to other issue areas. For example, the importance of countering child exploitation is already a matter of broad international agreement,[107] and swift progress on combating it may be possible by working to ensure that law enforcement can rapidly obtain the digital evidence necessary to conduct child exploitation investigations, including identifying and rescuing children who are being abused. Other issues subject to broad international rapprochement and interest, such as the use of the Internet by international terrorist organization or domain specific matters like the Anti-Money Laundering (AML), are potential areas for establishing an issue-specific, harmonized international data flow control framework. Starting with issues of broad consensus can provide an initial basis for subsequent bilateral or multilateral efforts to expand a harmonized framework to other forms of proscribed activity, or where there is otherwise a shared interest in establishing harmonized data flow mechanisms.

Of course, critical to all these efforts will be sequencing. Most likely, agreement amongst like-minded countries with similar legal regimes (as is the case with negotiations on a U.K.-U.S. Bilateral Agreement on Data Access) will need to precede agreements with more divergent worldviews. For instance, the United States, United Kingdom, Canada, Australia, and New Zealand, given

their similar legal regimes and history of close partnership, could reach agreement on a common framework for data flow controls, and then expand the set of countries committed to this common framework.[108]

At the same time, there may also be opportunities to start negotiations between countries that often do not see eye-to-eye. For instance, the 2013 agreement between U.S. President Barack Obama and Chinese Premier Xi Jinping limiting government-enabled theft of intellectual property, which appears to have had some success,[109] could provide a useful example of how agreement between the largest and most powerful global actors can establish norms that can be expanded to other countries. In all cases, issue selection and sequencing will necessarily depend upon the political and policy environments at play.

ADDITIONAL CHALLENGES

This paper identified the central challenge to transnational data flow controls—the lack of a harmonized international framework—and provided recommendations for how the international community might work towards a more harmonized system. However, additional issues remain. Chief among them is the question of cooperation between major technology providers and national law enforcement and regulators.

In order to ensure that governments are able to effectively enforce their laws and regulations, a reasonable level of cooperation between government agencies and companies is essential. The reality is that absent effective cooperation, governments are far more likely to implement laws and regulations that risk greatly impeding the growth and potential of the information economy. This risk is most substantial in nations where domestic commercial interests align with the imposition of strict rules and requirements on large, often foreign, providers. Accordingly, governments and providers alike must cooperate on a range of issues impacting global data flows, including on such matters as encryption, provider compliance with court orders, and the question of retention and provision of data to law enforcement. Multinational providers will undoubtedly face challenges in doing this, as their services are used by highly diverse communities and cultures, requiring them to understand the societal and legal norms in the jurisdictions in which they operate and to make appropriate accommodations. However, providers that do not make reasonable accommodations are more likely to be adversely impacted by laws or regulations that seek to compel them to take actions to abide by local norms. This is particularly the case when providers are unable to propose reasonable compliance alternatives to local authorities.

Further, while harmonizing data flow controls is clearly important to the future of the Internet and the information economy, it remains unclear precisely how important this issue is within the intersecting policy questions of trade, cybersecurity, and differing notions of appropriate state control of activities occurring in cyberspace (so called, "cyber sovereignty"). It is thus critical that governments, companies, and concerned citizens work to identify where and how data jurisdiction questions might be most effectively raised within multilateral or bilateral negotiations, or within debates about broader matters of international cooperation. Finding the right venues, the right cultural and diplomatic approaches to politically sensitive questions, and the most suitable timings for all these discussions will be essential, as the international community seeks to make progress on these most pressing policy questions.

CONCLUSION

We hope this paper has demonstrated that the current approaches to international data flow controls and the geographic-based framework for data jurisdiction are failing and need dramatic reworking. We have aimed to make the case that the solution to the problem lies in the harmonization of international data flow controls based upon flexible modes of cooperation between states and companies, without using the location of data as a primary consideration. The task is for governments, technology companies, civil society groups, and academia to foster shared global norms for appropriate data flow controls and to inject those shared principles into domestic law and policy, as well as international agreements. Absent such an effort, the situation will only become more intractable, jeopardizing the Internet's continued potential as a platform for communication, innovation, and commerce.

We recognize the many challenges at hand, yet we believe the international community today has an opportunity to begin the process of harmonizing data flow controls around a common framework and common set of standards. By doing so, the world can help preserve an Internet that spurs innovation and grows the economy; an Internet that allows the world to freely communicate across borders, thus advancing the fundamental human right, enshrined in Universal Declaration of Human Rights, "to seek, receive and impart information and ideas through any media and regardless of frontiers."[110] That is a goal we believe is worth striving towards.

Endnotes

1 For more background on how information is stored and distributed on the Internet, see The Harvard Law National Security Research Group (Ivana Deyrup, Shane Matthews, Aatif Iqbal, Benjamin Black, Catherine Fisher, John Cella, Jonathan Abrams, Miranda Dugi, & Rebecca Leventhal), "Cloud Computing and National Law," available at: https://lawfare.s3-us-west-2.amazonaws.com/staging/s3fs-public/uploads/2010/10/Cloud-Final.pdf; and Dillion Reisman, "Where Is Your Data, Really?: The Technical Case Against Data Localization", Lawfare (22 May 2017), available at: https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization

2 Indeed some argue that the existing Westphalian model of State territorial dominion is outmoded by the Internet. See Barlow, John Perry, "A Declaration of the Independence of Cyberspace" (8 February 1996). Available at: https://www.eff.org/cyberspace-independence; See also, Chris C. Demchak, Peter Dombrowski, "Rise of a Cybered Westphalian Age", (Spring 2011), Strategic Studies Quarterly. Available at: http://www.au.af.mil/au/ssq/2011/spring/demchak-dombrowski.pdf

3 Desai, Deven R., "Beyond Location: Data Security in the 21st Century", (December 3, 2012). Communications of the ACM, Vol. 56, January 2013. Available at: https://ssrn.com/abstract=2237712

4 We use the phrase "data flow controls" to refer to the broad set of state actions that affect the flow of data, including prohibitions on certain data, retention requirements, or production requirements.

5 Clark, David D., "Control Point Analysis", 2012 TRPC (10 September 2012). Available at: https://ssrn.com/abstract=2032124 or http://dx.doi.org/10.2139/ssrn.2032124

6 Helen Nissenbaum, *Privacy In Context: Technology, Policy, And The Integrity Of Social Life*, Stanford University Press (2009).

7 Drake, William J., Cerf, Vinton G., and Kleinwächter, Wolfgang, "Internet Fragmentation: An Overview", World Economic Forum (January 2016). Available at: http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf; Hill, Jonah Force. "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policy Makers", Paper, Science, Technology, and Public Policy Program, Belfer Center, Harvard Kennedy School of Government (May 2012). Available at: http://www.belfercenter.org/sites/default/files/legacy/files/internet_fragmentation_jonah_hill.pdf

8 Manyika, et al., "Global flows in a digital age: How trade, finance, people, and data connect the world economy", McKinsey Global Institute (April 2014). Available at: http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age

9 Hamilton, Alexander, Federalist Paper No. 15, "The Insufficiency of the Present Confederation to Preserve the Union".

10 For examples of the range of cross-border crimes enabled by the Internet, see the European Police Office's "2016 Internet Organized Crime Threat Assessment (IOCTA)". Available at: https://www.europol.europa.eu/activities-services/main-reports/internet-organised-crime-threat-assessment-iocta-2016

11 For example, see the Mutual Legal Assist Treaty Between the United States of America and the United Kingdom of Great Britain and Northern Ireland, signed January 6, 1994. Available at https://www.state.gov/documents/organization/176269.pdf

12 Krishnamurthy, Vivek, "Cloudy with a Conflict of Laws", (February 16, 2016). Berkman Center Research Publication No. 2016-3. Available at: https://ssrn.com/abstract=2733350

13 U.S. Department of Justice, "FY 2015 Budget Request: Mutual Legal Assistance Treaty Process Reform", (July 2014). Available at: https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf

14 Access Now, "Mutual Legal Assistance Treaties" (Accessed 9 July 2017). Available at: https://mlat.info/mlat-index

15 President's Review Group on Intelligence and Communications Technologies, "Liberty and Security in a Changing World" (12 December 2013). Available at: https://obamawhitehouse.archives.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

16 Krishnamurthy Ibd.

17 For more on the challenges posed by the block-features of ECPA, See: Woods, Andrew, "The Simplest Cross-Border Fix: Removing ECPA's Blocking Features", Lawfare (15 June 2017). Available at: https://www.lawfareblog.com/simplest-cross-border-fix-removing-ecpas-blocking-features.

18 Other provisions of ECPA prohibit companies from voluntarily disclosing "stored communications" to governments (U.S. and ex-U.S) absent specified exceptions. 18 U.S.C. 2702.

19 David Anderson Q.C., "A Question of Trust: Report of the Investigatory Powers Review" (June 2015). Available at: https://terrorismlegislationreviewer.independent.gov.uk/wp-content/uploads/2015/06/IPR-Report-Print-Version.pdf

20 Paulo Marcos Rodriguez Brancher and Douglas Cohen Moreira, "Brazilian Superior Court of Justice decision and the disclosure of Gmail data for investigation", Lexology (29 April 2013). Available at http://www.lexology.com/library/detail.aspx?g=793d848f-5877-4675-9336-aa28eec3d971 (Accessed12 June 2014); Rebecca Blumenstein and Loretta Chao, "Brazil's Rousseff Pressures U.S. on Data Collection", *The Wall Street Journal* (25 January 2014) Available at: https://www.wsj.com/articles/brazil8217s-rousseff-pressures-us-on-data-collection-1390604047?tesla=y

21 "MLATS and International Cooperation for Law Enforcement Purposes", presentation at the Centre for Internet and Society. Available at: https://cis-india.org/internet-governance/blog/presentation-on-mlats.pdf

22 Matter of Warrant to Search a Certain E-Mail Account Controlled & Maintained by Microsoft Corp., 829 F.3d 197 (2d Cir. 2016)

23 For more on Microsoft's perspective, see the blog post by Brad Smith, "A legislative path to create new laws is better than arguing over old laws", Microsoft Blog (23 June 2017). Available at: https://blogs.microsoft.com/on-the-issues/2017/06/23/legislative-path-create-new-laws-better-arguing-old-laws/

24 Supra 829 F.3d 197 (2d Cir. 2016)

25 On 28 June 2017, the Department of Justice petitioned the Supreme Court of the U.S. to hear this case. U.S. Department of Justice, "In The Matter Of A Warrant To Search A Certain E-mail Account Controlled And Maintained By Microsoft Corporation" (28 June 2017). Available at: https://www.justice.gov/sites/default/files/briefs/2017/06/28/17-2_microsoft_corp_petiton.pdf

26 *United States v. Microsoft Corp.*, Docket #17-2, "Whether a United States provider of email services must comply with a probable-cause-based warrant issued under 18 U.S.C. § 2703 by making disclosure in the United States of electronic communications within that provider's control, even if the provider has decided to store that material abroad". Available at: https://www.supremecourt.gov/docket/docketfiles/html/public/17-2.html

27 Counsel for Amicus Curiae Ireland, "Brief Of Amicus Curiae Ireland in 14-2985-CV" (23 December 2014). Available at: https://www.eff.org/files/2015/01/12/ireland_microsoft_second_circuit_amicus_brief.pdf

28 Littlehale, Richard, testimony before the U.S. House of Representatives Committee on the Judiciary, hearing on "Data Stored Abroad: Ensuring Lawful Access and Privacy Protection in the Digital Era" (15 June 2017). Available at: https://judiciary.house.gov/hearing/data-stored-abroad-ensuring-lawful-access-privacy-protection-digital-era/

29 Littlehale, Richard, Ibid.

30 For a brief introduction to data sharding see: Microsoft, "Sharding Pattern" (23 June 2017). Available at: https://docs.microsoft.com/en-us/azure/architecture/patterns/sharding

31 Wall, Jeffrey, "Reply Brief for the United States. In the Matter of a Warrant to Search a Certain E-Mail Account Controlled and Maintained By Microsoft Corporation" (September 2017). Available at: https://arstechnica.com/wp-content/uploads/2017/09/scotusmsftgoogyahoo.pdf. Additionally, see In re Search Warrant No. 16-960-M-1 to Google (E.D. Pen. Aug. 17, 2017); In re Search of Content that Is Stored at Premises Controlled by Google Inc. and as Further Described in Attachment A, No. 16-mc-80263 (N.D. Cal. Aug. 14, 2017), aff'g 2017 WL 1487625 (N.D. Cal. Apr. 25, 2017); In re Search of Info. Associated with [Redacted]@gmail.com that Is Stored at Premises Controlled by Google, Inc., No. 16-mj-757, 2017 WL 3445634 (D.D.C. July 31, 2017), aff'g 2017 WL 2480752 (D.D.C. June 2, 2017); In re Search of Info. Associated with Accounts Identified as Redacted]@gmail.com and Others Identified in Attachment A that Are Stored at Premises Controlled by Google Inc., No. 16-mj-2197, 2017 WL 3263351 (C.D. Cal. July

13, 2017); In re Search Warrant to Google, Inc., Mag. No. 16-4116, 2017 WL 2985391 (D.N.J. July 10, 2017) (objections filed); In re Two Email Accounts Stored at Google, Inc., No. 17-M-1235, 2017 WL 2838156 (E.D. Wisc. June 30, 2017) (objections filed); In re Search of Premises Located at Redacted]@yahoo.com, No. 17-mj-1238 (M.D. Fla. Apr. 7, 2017); In re Search Warrant No. 16-960-M-01 to Google, 232 F. Supp. 3d 708 (E.D. Pa. Feb. 3, 2017).

32 In contrast, search warrants usually require specifying the location to be searched, which is a significant legal constraint on the scope of U.S. law enforcement's power.

33 It can be argued that since the U.S. entered into the majority of its existing MLATs prior to the advent of the cross-border data flow phenomenon, that MLATs are further unsuited to be the answer to the challenges presented by the need to balance operational efficiency in law enforcement with a considered decision based upon on the merits of a particular form of process, to say nothing of a government's entire system for the issuing process.

34 See, e.g., CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders, U.S. Dep't of Just., Comput. Crime & Intell. Prop. Section (6 June 2016). Available at: https://www.csis.org/events/ccips-csis-cybercrime-symposium-2016. As an additional example see: The "Cross-Border Requests for Data Project" at the Institute for Information Security and Privacy at Georgia Tech (http://www.iisp.gatech.edu/cross-border-data-project). Also, the Dutch Presidency of the European Union convened the "Crossing Borders: Jurisdiction in Cyberspace" conference in Amsterdam on 6-7 March 2016.

35 For instance, Peter Swire and Justin Hemmings of Georgia Tech have suggested that a streamlined MLAT system could be possible through statutory changes akin to the current Visa Waiver Program. They argue that eligible countries with high-quality procedures for seeking evidence would be eligible for a streamlined process for obtaining evidence in the United States, in much the same way that certain countries are exempted from background checks for visas. See, Swire, Peter and Hemmings, Justin D., "Mutual Legal Assistance in an Era of Globalized Communications: The Analogy to the Visa Waiver Program" (11 January 2016), 71 NYU Annual Survey of American Law 687 (2017); Georgia Tech Scheller College of Business Research Paper No. WP 38. Available at SSRN: https://ssrn.com/abstract=2728478 or http://dx.doi.org/10.2139/ssrn.2728478

36 Two notable examples are the "Law Enforcement Access to Data Stored Abroad Act" (LEADS Act), available at: https://www.congress.gov/114/bills/hr1174/BILLS-114hr1174ih.xml, and the "International Communications Privacy Act " (ICPA), available at https://www.congress.gov/114/bills/s2986/BILLS-114s2986is.xml

37 In the United Kingdom, the Parliament has passed the Investigatory Powers Act which greatly expands the extraterritorial reach of British law enforcement, allowing for expansive "equipment interference," or hacking of computers, outside of U.K. territory. Home Office of the United Kingdom, "Equipment Interference, DRAFT Code of Practice" (Fall 2016). Available at, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/557861/IP_Bill_-_Draft_EI_code_of_practice.pdf. Additionally, the government of Ethiopia was alleged, in a U.S. civil case, to have used FinSpy to gather information from a U.S. citizen's electronic devices located in the United States. Interestingly, the U.S Court of Appeals for the District of Columbia Circuit ruled that the Foreign Sovereign Immunities Act (FSIA) provided the government of Ethiopia immunity from such a lawsuit. See Doe v. Fed. Democratic Republic of Ethiopia, No. 16-7081, 2017 U.S. Appl. LEXIS 4414.

38 Hennessey, Susan and Mirasola, Chris, "Did China Quietly Authorize Law Enforcement to Access Data Anywhere in the World?", Lawfare (27 March 2017). Available at: https://www.lawfareblog.com/did-china-quietly-authorize-law-enforcement-access-data-anywhere-world

39 Daum, Jeremy, "Sometimes a rule of evidence is just a rule of evidence", China Law Translate (29 March 2017). Available at: http://www.chinalawtranslate.com/sometimes-a-rule-of-evidence-is-just-a-rule-of-evidence/?lang=en

40 In the Fall of 2017, it was alleged that China hacked the law firm representing a Chinese dissident who is located in and seeking asylum from the U.S., see: Gertz, Bill "FBI Eyes China in Posting Hacked Documents on Chinese Dissident", *The Washington Free Beacon* (29 September 2017). Available at: http://freebeacon.com/national-security/fbi-eyes-china-posting-hacked-documents-chinese-dissident/

41 Federal Rules of Criminal Procedure, 41(b)(6). For further discussion, see: https://www.justice.gov/archives/opa/blog/rule-41-changes-ensure-judge-may-consider-warrants-certain-remote-searches

42 For example, see: http://www.tandfonline.com/doi/full/10.1080/00396338.2016.1231534; http://scholarlycommons.law.northwestern.edu/cgi/viewcontent.cgi?article=1209&context=njtip; https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2633247

43 According to joint testimony of the Honorable Clapper, the Honorable Lettre, and Admiral Rogers, more than 30 countries are developing offensive cyber attack capabilities (see https://www.armed-services.senate.gov/imo/media/doc/Clapper-Lettre-Rogers_01-05-16.pdf).

44 For more on the potential risks related to "lawful hacking" we recommend this paper by Orin Kerr and Sean Murphy "Government Hacking to Light the Dark Web" (July 2017). Available at: https://www.stanfordlawreview.org/online/government-hacking-to-light-the-dark-web/

45 McQuinn, Alan and Castro, Daniel, "How Law Enforcement Should Access Data Across Borders", Information Technology & Innovation Foundation (July 2017). Available at: http://www2.itif.org/2017-law-enforcement-data-borders.pdf

46 For example, consider the recent U.S. criminal case involving the Bitcoin Exchange BTC-e; in this case, you had a web service with obscured ownership, unknown data storage location, yet was a service used by criminals throughout the world for a wide range of crimes. For more on the BTC-E case, see: https://www.justice.gov/usao-ndca/pr/russian-national-and-bitcoin-exchange-charged-21-count-indictment-operating-alleged

47 Rosenzweig, Paul, "The US-UK Deal Is Actually Quite Good", Lawfare (19 July 2017). Available at: https://lawfareblog.com/us-uk-deal-actually-quite-good

48 Written Testimony of Mr Paddy McGuinness, United Kingdom Deputy National Security Adviser, Before the Judiciary Sub-Committee on Crime and Terrorism United States Senate (May 10, 2017). https://www.judiciary.senate.gov/imo/media/doc/05-24-17%20McGuinness%20Testimony.pdf

49 ECPA was enacted to provide additional protections for electronic communications, beyond those provided by the Fourth Amendment to the U.S. Constitution; its provisions (18 U.S.C. §§ 2510-2522, 2701-2712, 3121-3127) impose broad prohibitions on electronic communications providers disclosing communications information except for in specified circumstances. For more on the blocking aspects of ECPA, see the written Testimony of Andrew Keane Woods before the House Judiciary Committee (15 June 2017). Available at: https://judiciary.house.gov/wp-content/uploads/2017/06/Woods-Testimony.pdf.

50 For more on the framework for allowing for cross-border data requests, see the various works of Jennifer Daskal and Andrew Keane Woods; for example: https://lawfareblog.com/cross-border-data-requests-proposed-framework.

Also of note is the International Communications Privacy Act (ICPA), proposed by Senators Hatch, Coons, and Heller on 1 August 2017, which primarily focuses on the citizenship and location of the suspects, rather than the location data may be stored or even who controls that data. The text of ICPA is available at: https://www.congress.gov/bill/115th-congress/senate-bill/1671/cosponsors. It bears note that any comparison of national legal orders to determine "compatibility" in this context is an exceptionally complex undertaking, and attempts to do so have almost universally been subject to reasonable critique regarding the politicization of their conclusions.

51 For example, see Prince, Matthew, "Why We Terminated Daily Stormer", Cloudflare (16 August 2017). Available at: https://blog.cloudflare.com/why-we-terminated-daily-stormer/

52 Court of Appeal for British Columbia, *Equustek Solutions Inc. v. Google Inc.*, 2015 BCCA 265. Available at: https://www.canlii.org/en/bc/bcca/doc/2015/2015bcca265/2015bcca265.pdf

53 Google v. Equustek Solutions Inc. U.S. District Court of Northern District of California San Jose Division. Available at: https://assets.documentcloud.org/documents/3900043/Google-v-Equustek-Complaint.pdf

54 Woods, Andrew, "Google Takes the Global Delisting Debate to a U.S. Court", Lawfare (27 July 2017). Available at: https://www.lawfareblog.com/google-takes-global-delisting-debate-us-court

55 For example, see: http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally; https://www.eff.org/cases/google-v-equustek; https://blog.wikimedia.org/2016/10/14/intervention-google-v-equustek; https://www.washingtonpost.com/news/volokh-conspiracy/wp/2017/06/29/canadian-court-orders-google-to-remove-search-results-globally

56 Woods, Andrew, "No, the Canadian Supreme Court Did Not Ruin the Internet", Lawfare (6 July 2017). Available at: https://www.lawfareblog.com/no-canadian-supreme-court-did-not-ruin-internet

57 Keller, Daphne, "Ominous: Canadian Court Orders Google to Remove Search Results Globally", Center for Internet and Society (28 June 2017). Available at: http://cyberlaw.stanford.edu/blog/2017/06/ominous-canadian-court-orders-google-remove-search-results-globally

58 For a summary, see "Google Spain SL v. Agencia Española de Protección de Datos", Harvard Law Review (13 May 2014). Available at: https://harvardlawreview.org/2014/12/google-spain-sl-v-agencia-espanola-de-proteccion-de-datos/

59 Council Directive 95/46, 1995 O.J. (L 281) 31 (EC).

60 Farhad Manjoo, "'Right to Be Forgotten' Online Could Spread," *New York Times*, 15 August 2015.

61 Ibid.

62 Fleischer, Peter "Adapting our approach to the European right to be forgotten", Google (4 March 2016). Available at: https://www.blog.google/topics/google-europe/adapting-our-approach-to-european-rig

63 Walker, Kent, "A principle that should not be forgotten", Google (19 May 2016). Available at: https://www.blog.google/topics/google-europe/a-principle-that-should-not-be-forgotten

64 For example, see: https://www.wsj.com/articles/google-wages-free-speech-fight-in-mexico-1432723483; https://advox.globalvoices.org/2014/09/18/right-to-be-forgotten-a-win-for-argentinas-lawsuit-happy-celebrities

65 Lim, James, "South Korea Releases Right to Be Forgotten Guidance", *Bloomberg BNA* (9 May 2016). Available at: https://www.bna.com/south-korea-releases-n57982070847

66 See, Sidley Austin LLP, "Essentially Equivalent: A Comparison of the Legal Orders for Privacy and Data Protection in the European Union and United States", (25 January 2016). Available at: https://www.sidley.com/en/insights/publications/2016/01/essentially-equivalent

67 Rosenzweig, Paul, "Europe Is Deeply Unserious", Lawfare (27 July 2017). Available at: https://www.lawfareblog.com/europe-deeply-unserious

68 Personal Data Protection Law Draft Bill - Brazil. As published for public comment by the Executive Branch on 28 January 2015, available at : https://iapp.org/media/pdf/resource_center/Brazil_PDPL_Draft_Bill-final.pdf; https://uk.practicallaw.thomsonreuters.com/4-520-1732

69 Chinese National People's Congress, "People's Republic of China Internet Security Law" (7 November 2016). Available at: http://www.npc.gov.cn/npc/xinwen/2016-11/07/content_2001605.htm

70 Russian Federal Law No. 242-FZ, "On making amendments to certain laws of the Russian Federation regarding clarification of the order of processing of personal data in information and telecommunication networks".

71 See, Judgment in Case C-362/14 Maximillian Schrems v Data Protection Commissioner, Luxembourg, (6 October 2015). Available at https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-10/cp150117en.pdf

72 The invalidation of the EU-US Safe Harbor Agreement did not lead to a major fracturing of the Internet because governments, companies, and individual Internet users understood that a total stoppage of data flows to the United States would cripple the digital economy on both sides of the Atlantic. The U.S. and the E.U. were able to (1) ensure that European Data Protection Authorities provided a grace period for transition to the use of other instruments to permit data transfers, such as the execution of contracts based on the European Commission's approved Standard Contractual Clauses, and perhaps more impactfully (2) successfully negotiate and implement a new agreement, the EU-US Privacy Shield Arrangement, which when paired with the Judicial Redress Act, a law passed in 2016 by the U.S. Congress and signed into law by President Obama, provided additional safeguards and redress mechanisms for EU citizens concerned about the privacy of their data transferred to the United States. Interestingly, despite the close attention to "data protection" in the United States and critical commentary as compared to the European Union's own regime, there has been comparatively little attention to the "adequacy" of other countries to which the European Union regularly transfers data, including notably the People's Republic of China. Indeed, the Directorate-General for Internal Policies stated in a 2015 report to the European Parliament Committee on Civil

Liberties, Justice and Home Affairs (LIBE) notes this tension, acknowledging "one cannot talk of a proper data protection regime in China...even if one chooses to disregard the human rights parameter for sake of analysis...the basics of international data protection are not unequivocally in place in China today." See European Parliament Directorate-General for Internal Policies, The data protection regime in China: In-depth Analysis for the LIBE Committee (Oct. 2015). Available at http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

73 For a comprehensive list of restrictions, see Cory, Nigel. "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" Information Technology and Innovation Foundation (ITIF), May 2017. Available at http://www2.itif.org/2017-cross-border-data-flows.pdf?_ga=2.244607109.1624330899.1511348753-1808609825.1511348753

74 Hill, Jonah Force. "The Growth of Data Localization Post-Snowden", Lawfare Research Paper Series (21 July 2014). Available at: https://www.lawfareblog.com/jonah-force-hill-growth-data-localization-post-snowden-lawfare-research-paper-series

75 The New York County District Attorney's Office, "Ensuring Lawful Access to Smartphones" (13 June 2017). Available at: http://manhattanda.org/smartphone-encryption

76 Importantly, data localization requirements are also often viewed by lawmakers—incorrectly—as kind of panacea for cybersecurity challenges. But as with privacy, the physical location of data has little to no impact on security.

77 Other countries, most notably Estonia, are considering anti-localization strategies, seeking to ensure their countries' data is stored abroad and under the protection of foreign partners. Estonia Ministry of Economic Affairs and Communications and Microsoft, "Implementation of the Virtual Data Embassy Solution". Available at: https://www.mkm.ee/sites/default/files/implementation_of_the_virtual_data_embassy_solution_summary_report.pdf

78 Again, our advocacy for this approach should not imply that what is needed is a new all-encompassing international treaty or another single international legal mechanism. The chances of success of such a treaty are low in light of the number of governments and other actors that would be impacted and thus need to be involved in the process. Rather, we suggest rethinking prior notions of geography as a basis for jurisdiction as a means of beginning to develop new mechanisms of cooperation.

79 Jack Goldsmith and Tim Wu, *Who Controls the Internet?: Illusions of a Borderless World*, Oxford University Press, Inc., New York, NY, USA (2006).

80 Clark, David D., "Control Point Analysis", 2012 TRPC (September 10, 2012). Available at SSRN: https://ssrn.com/abstract=2032124 or http://dx.doi.org/10.2139/ssrn.2032124

81 Similarly, the Electronic Frontier Foundation (EFF) applies a control point analysis to illustrate potential constraints to speech on the Internet. The EFF's depiction of the control points involved in web communication is available at: https://www.eff.org/free-speech-weak-link

82 Helen Nissenbaum, *Privacy In Context: Technology, Policy, And The Integrity Of Social Life*, Stanford University Press (2009).

83 Nissenbaum, Helen, "Privacy as Contextual Integrity," *Washington Law Review* (2004). Available at: https://crypto.stanford.edu/portia/papers/RevnissenbaumDTP31.pdf

84 This factor encompasses the "sender" and "recipient" factors of CIM, while also including various entities involved in content distribution: hosters, domain registrars, ISPs, etc.

85 This factor encompasses the "information type" factor of CIM, while recognizing that there is a potentially far greater set of defined types of data in the broad context of data controls compared to privacy controls.

86 This factor encompasses both the "transmission principles" and "subject" factors of CIM. We agree that subjects are a particularly relevant factor in considering privacy protections, however, in the broad set of data flow controls, we consider them one amongst many with various rights to the data (for example, the creator or copyright holder).

87 APEC Secretariat, "APEC Privacy Framework 2015". Available at: http://www.cbprs.org/

88 Ibid.

89 Ibid.

90 Ibid.

91 For more information see: https://www.un.org/disarmament/topics/informationsecurity

92 Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era", Google Blog (22 June 2017). Available at: https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf

93 Ibid.

94 For more on the Internet and Jurisdiction Policy Network, see: https://www.internetjurisdiction.net

95 The goal of the I&J is to "catalyze the development of shared cooperation frameworks and policy standards that are as transnational as the Internet itself in order to promote legal interoperability and establish due process across borders."

96 "Location of the physical carriers of the information to be accessed as a criteria for jurisdiction and proxy for control has a long legal history. However, the connection is harder to make in the age of cloud-based storage. There would be a strong benefit in moving away from this criteria and replacing it by the notion of control of the data. A proper regime should establish the conditions of access to evidence in the cloud, irrespective of where it is physically stored. Special attention needs to be paid to the chain of custody of the data: cloud operators often provide back-end capacity to other services that exercise the actual control over the data being sought. As custodian, the cloud provider should be tasked with channeling the requests to this ultimate recipient rather than be asked to communicate data that it does not directly control. This of course introduces additional complexities given the number of potential jurisdictions involved." See, Data and Jurisdiction Program, Cross Border Access to User Data, Problem Framing, May 2017. Available at https://www.internetjurisdiction.net/uploads/pdfs/Papers/Data-Jurisdiction-Program-Paper.pdf

97 See the APEC CBPR system, available at: http://www.cbprs.org

98 The eCommerce Chapter of TPP provides a useful example of how data flow standards can be incorporated into a trade agreement. See the 2016 negotiated language at https://ustr.gov/sites/default/files/TPP-Final-Text-Electronic-Commerce.pdf

99 For a discussion of counter-data localization provisions in trade agreements, see William J. Drake, "Background Paper for the workshop on Data Localization and Barriers to Transborder Data Flows", 14-15 September 2016, The World Economic Forum, Geneva. Available at: http://www3.weforum.org/docs/Background_Paper_Forum_workshop%2009.2016.pdf

100 Convention on the Recognition and Enforcement of Foreign Arbitral Awards (New York, 1958) (the "New York Convention") http://www.uncitral.org/uncitral/en/uncitral_texts/arbitration/NYConvention.html

101 For instance, the Doha Development Round, the latest trade negotiation round of the World Trade Organization, has been ongoing since 2011 and has not yet been completed.

102 See, Statement of David Bitkower, Principal Deputy Assistant Attorney General, Criminal Division, U.S. Department of Justice, before the Committee on the Judiciary, United States House of Representatives (25 February 2016). Available at https://www.justice.gov/opa/file/828686/download

103 Smith, Brad, "A legislative path to create new laws is better than arguing over old laws", Microsoft (23 June 2017). Available at: https://blogs.microsoft.com/on-the-issues/2017/06/23/legislative-path-create-new-laws-better-arguing-old-laws; https://www.judiciary.senate.gov/meetings/law-enforcement-access-to-data-stored-across-borders-facilitating-cooperation-and-protecting-rights

104 Google, "Digital Security & Due Process: Modernizing Cross-Border Government Access Standards for the Cloud Era", Blog Post (22 June 2017). Available at: https://www.blog.google/documents/2/CrossBorderLawEnforcementRequestsWhitePaper_2.pdf; https://judiciary.house.gov/wp-content/uploads/2017/06/Salgado-Testimony.pdf

105 For additional discussion of this proposal see, Paul Rosenzwieg, "The US-UK Deal Is Actually Quite Good", Lawfare (19 July 2017). Available at: https://www.lawfareblog.com/us-uk-deal-actually-quite-good

106 European Commission, "Questionnaire on improving criminal justice in cyberspace: Summar of Response." Available at: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/e-library/documents/policies/organized-crime-and-human-trafficking/e-evidence/docs/summary_of_replies_to_e-evidence_

questionnaire_en.pdf

107 WePROTECT, "The WePROTECT Global Alliance", (12 July 2016). Available at: http://www.weprotect.org/strategylaunch

108 However, it can be argued that even if such approaches could be extended to these countries, that the underlying international tensions would not be defrayed to a sufficient degree to address the real concerns until all of the "major markets" in which U.S. tech companies have a significant presence have been given a workable solution.

109 "The cybersecurity company FireEye released a report in June 2016 that claimed the the number of network compromises by the China-based hacking groups it tracks dropped from 60 in February 2013 to less than 10 by May 2016." See the Council on Foreign Relations blog, "The U.S.-China Cyber Espionage Deal One Year Later," September 2016. Available at https://www.cfr.org/blog/us-china-cyber-espionage-deal-one-year-later

110 "Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers." Article 19, Universal Declaration of Human Rights