ITIF | INFORMATION TECHNOLOGY & INNOVATION FOUNDATION

Principles and Policies for "Data Free Flow With Trust"

NIGEL CORY , ROBERT D. ATKINSON, AND DANIEL CASTRO | MAY 2019

The foundation of the global digital economy is showing cracks. Countries that support an open, rules-based global trading system need to agree on a common framework.

KEY TAKEAWAYS

- The digital economy's foundation is cracking as some countries try to impose their rules on others, and some erect barriers and turn inward.
- To maximize the innovation and productivity benefits of data, countries that support an open, rules-based trading system need to agree on core principles and common rules.
- Rather than tell firms where they can store or process data, countries should hold firms accountable for managing data they collect, regardless of where they store or process it.
- Countries should revise inefficient processes and outdated legal agreements governing law enforcement access to data stored in other jurisdictions.
- Countries should adopt policies with appropriate checks and balances for ISPs to block data flows involving illegal distribution of unlicensed content.
- For data to flow "with trust," countries must support the key technology people and businesses rely on to ensure its confidentiality: encryption.

OVERVIEW

Just as there was a set of institutions, agreements, and principles that emerged out of Bretton Woods in the aftermath of World War II to manage global economic issues, the countries that value the role of an open, competitive, and rules-based global digital economy need to come together to enact new global rules and norms to manage a key driver of today's global economy: data. Japanese Prime Minister Abe's new initiative for "data free flow with trust," combined with Japan's hosting of the G20 and leading role in e-commerce negotiations at the World Trade Organization (WTO), provides a valuable opportunity for many of the world's leading digital economies (Australia, the United States, and European Union, among others) to rectify the gradual drift toward a fragmented and less-productive global digital economy. Prime Minister Abe is right in proclaiming, "We have yet to catch up with the new reality, in which data drives everything, where the D.F.F.T., the Data Free Flow with Trust, should top the agenda in our new economy," and right in his call "to rebuild trust toward the system for international trade. That should be a system that is fair, transparent, and effective in protecting IP and also in such areas as e-commerce."[1.]

The central premise of this effort should be a recognition that data and data-driven innovation are a force for good.[2] Across society, data innovation—the use of data to create value—is creating more productive and innovative economies, transparent and responsive governments, better social outcomes (improved health care, safer and smarter cities, etc.).[3] But to maximize the innovative and productivity benefits of data, countries that support an open, rules-based global trading system need to agree on core principles and enact common rules. The benefits of a rules-based and competitive global digital economy are at risk as a diverse range of countries in various stages of political and economic development have policy regimes that undermine core processes, especially the flow of data and its associated legal responsibilities; the use of encryption to protect data and digital activities and technologies; and the blocking of data constituting illegal, pirated content.

To maximize the innovative and productivity benefits of data, countries that support an open, rules-based global trading system need to agree on core principles and enact common rules.

Japan's hosting of the G20 provides a valuable forum for discussions of these issues, as it involves many key players and comes at a (long-overdue) moment when countries are moving toward new rules and norms, both domestically and internationally, that impact the global digital economy. This report outlines the Information Technology and Innovation Foundation's (ITIF's) views on some of the core principles, rules, and issues that should be on the agenda. The report starts with a brief overview of ITIF's framework for cross-border Internet policy. This provides the foundation for four key principles and policies ITIF recommends policymakers consider as part of discussions on data free flow with trust and related issues and initiatives at WTO and other forums.

These principles and policies are:

1. **Rather than tell firms where they can store or process data, policymakers should hold firms accountable for managing data they collect, regardless of where they store or process it.** Leading digital economies need to articulate and enact a framework that is based on local accountability and interoperability in order to provide a clearer, and better, alternative to the two other main, contrasting approaches: efforts by (mainly European) countries to make other countries adopt their (universalist) approach to data privacy in order to make them responsible for enforcement (instead of holding firms responsible), and countries forcing firms to only store data locally (a concept known as data localization).

    a. Similarly, policymakers should apply an accountability-based approach to ensuring firms provide timely access to data in response to requests for data from financial regulatory authorities, rather than focusing on the location of data storage.

2. **Countries should revise the inefficient processes and outdated legal agreements that govern law enforcement requests for access to data stored in another country's jurisdiction.** If we are to establish a widely shared free flow of data with trust regime, one key component of that trust needs to be national law enforcement agencies trusting they can get access to domestic data (related to legitimate law enforcement investigations) stored in other nations.

    a. Countries should develop a Geneva Convention for Data that would establish international rules for transparency, settle questions of jurisdiction, and increase cooperation and coordination of cross-border requests from law enforcement.

    b. Beyond new and ongoing initiatives (such as the U.S. Cloud Act executive agreements and EU e-evidence reforms), countries should also improve existing institutions, processes, and tools used to manage cross-border law enforcement requests for data, especially mutual legal assistance treaties (MLATs), to ensure requests are handled efficiently.

3. **Countries should develop the legal and administrative frameworks (with respective checks and balances) that allow Internet service providers to block data flows that involve the illegal distribution and use of unlicensed content.** Within the concept of data free flow with trust, it is important to recognize that not all data flows should be treated the same, as some data flows are rightly illegal. The world's leading digital economies should recognize that website blocking is a constructive intellectual property policy tool to use for copyright enforcement, as Australia, Singapore, the United Kingdom, and dozens of other countries already do.

4. **Countries should support and not undermine encryption's role in securing data flows and digital technologies.** For data to flow "with trust," as specified by Prime Minister Abe, it needs to take into consideration the key technology people and businesses rely on to ensure the confidentiality of data: encryption. Any government attempt to undermine encryption reduces the overall security of law-abiding citizens and businesses, makes it more difficult for companies from countries with weakened encryption to compete in global markets, and limits advancements in information security.

A PRAGMATIC GLOBAL FRAMEWORK TO ADDRESS CROSS-BORDER INTERNET POLICY

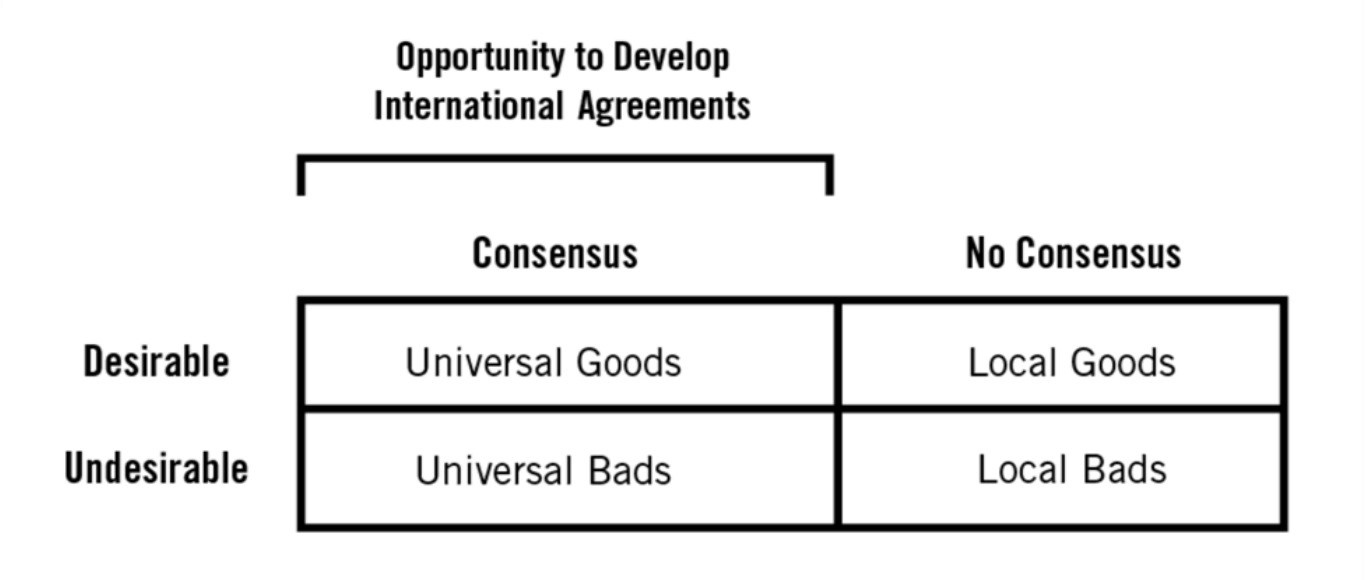
Countries have made little substantive progress in creating a framework for resolving the many conflicts over Internet policy that inevitably occur between sovereign nations sharing access to a global medium, despite the fact that the Internet grows more important to society and the global economy each day. These conflicts arise over a myriad of issues, such as free speech, intellectual property, privacy, cybercrime, consumer protection, taxation, commercial regulation, and others. To date, despite many attempts, no framework has been successful at providing a practical and widely accepted model for policymakers to resolve cross-border Internet policy conflicts in ways that respect both the global nature of the Internet and national laws and norms.

This means the Internet, like all other technologies, has ended up being guided by both formal and informal rules by international, national, and subnational bodies (whether government or nongovernment) throughout its history.[4] The result is an uncoordinated patchwork of laws, treaties, regulations, norms, and standards. These often come into conflict with each other, especially as policy decisions in one country can create significant negative externalities for individuals and businesses outside of that country—an effect not likely to be taken into consideration. Or a nation may pass a law that impacts firms and individuals outside of its jurisdiction and is simply unenforceable. From a trade and economic perspective, disputes over these policies and approaches can be used as cover for what are essentially anticompetitive, trade-distorting actions that harm the global economy. When this happens, many individuals and organizations can be caught in the middle.

A key reason for the lack of progress on global Internet policy is nations have different values and priorities, and attempts at resolving policy disputes inevitably falter because the various parties lack a common basis for dialogue. This leads to two generally opposed approaches: universalism and Balkanism. Regarding the former, a reason many proposed frameworks have failed is they try to apply a particular nation's worldview, such as promoting democracy and freedom of expression (as in the case of the United States), or maintaining political control (as in the case of nations such as China and Russia), on the rest of the world. However, some of the most fervent calls for universalism come from cyber-libertarian groups in the West who call for universal rules such as "Internet freedom for all," "no online censorship," and "an open Internet." These types of advocates generally call for government to not enact policies that effect the Internet.[5] But despite the appeal of these universal proposals (e.g., they would be relatively easy to administer if everyone would just agree to one universal framework, and an open Internet is a good thing), such frameworks simply cannot work because nations have significantly different cultural values, policy priorities, and legal systems. But the alternative—a Balkanized, fragmented global Internet that gives nations the right to act as they please on the web—cannot be the answer either.

Therefore, what is needed is a framework that allows nations the right to design Internet policy according to their own national needs and rules, avoid trampling on the rights of other sovereign nations, and develop common solutions to address issues where there is broad global consensus about desirable "universal goods" and undesirable "universal bads" (see figure 1).[6]

Figure 1: Typology of Internet policy goals affecting individuals outside the country [7]



The clearest example of a universal good, and thus the need for universal rules, pertains to frameworks on core Internet architecture and protocols, as the Internet needs commonly shared global standards. A multi-stakeholder approach to maintaining this goal is desirable, as debates and disagreements over the technical architecture and protocols of the Internet can only be

resolved with stakeholder consensus. And the Internet, which is itself a network of networks, has vastly more stakeholders, many of which are private companies, than previous telecommunications systems, so a multi-stakeholder model is best suited for such technical discussions.

An example of a universal good in how the Internet is used in countries that want to put in place new rules on digital trade, as they recognize the shared benefits of promoting an open, competitive, and innovative global digital economy. This is an extension of the basis for the existence of WTO, in that it provides evidence of broad international consensus on the benefits of free trade (a universal good). Similarly, as there is broad international agreement on the need to combat child pornography (a universal bad), including a United Nations human rights treaty, signatory nations should support Internet policies designed to reduce this and other criminal activity, such as digital content piracy.[8]

What is needed is a framework that allows nations the right to design Internet policy according to their own national needs and rules, avoid trampling on others' rights, and develop common solutions where there is broad global consensus about universal goods and bads.

However, countries need to recognize that when it comes to policies about how the Internet is used, as opposed to policies about how the Internet is constructed, there can be differences between nations. As shown in figure 1, these are local goods or local bads. Policymakers need to recognize this policy distinction—between policies with global consensus and those without—as they consider principles and policies pertaining to data free flow with trust. Given that the issues raised in this report involve the use of the Internet (and not its architecture), this consensus will (at best) be widespread but not unanimous. Some countries (most likely those authoritarian in nature) will not see international cooperation as desirable, as these countries associate data governance with political and social control. Therefore, these countries are likely to be intractable in coming up with principles and mechanisms that allow for cross-border data flows, robust encryption, and other measures that are part of a global framework for global digital activity.

Given this, it is better that a consensus-based approach be ambitious, but pragmatic, in seeking shared principles and agreements on selected data-related issues among a likeminded group of countries that together represent a substantial part of the global economy and value an open, rules-based, and innovative global digital economy. Policymakers need to consider the alternative if they continue to persevere (in vain) for some sort of harmonized, universalist outcome on data-related issues. While this takes place, more and more countries will enact restrictive data-related policies that make not only such an outcome less likely, but any such outcome increasingly ineffective—in terms of an open and competitive global digital economy—given where it would inevitably place the lowest common denominator among countries with the most restrictive approach to digital governance.

Australia, Japan, the United States, and other nations need to seize the opportunity to lead the agenda in forming a consensus on core principles, tools, and agreements on issues affecting the global digital economy, such as on the cross-border flow of data. These countries can pursue such rules in whichever forum and mechanism they see as the most appropriate (whether through WTO, bilaterally, or elsewhere), but the more they are able to start from a set of shared principles and preferred outcomes, the more likely they are to make progress. The subsequent sections outline four core principles and policies ITIF believes should be at the heart of Prime Minister Abe's initiative for data free flow with trust.

Principle 1: Firms Should Be Held Accountable for Managing the Data They Collect, Regardless of Where They Store, Process, or Transfer the Data

Accountability should be the principle at the heart of a global framework for the free flow of data with trust. When policymakers deal with data governance and cross-border data flows, the basic expectation should be that when it comes to handling data, companies doing business in a country should be responsible and held accountable under that nation's laws and regulations, for both their own actions and the actions of their agents and business partners, regardless of whether they're located inside or outside the country where a firm collects or manages data. Therefore, the focus for policymakers in making data-related laws and regulations is ensuring they hold firms accountable regardless of where the firms store, process, or transfer data.

This accountability principle is based on two key points: A firm with "legal nexus" in a country's jurisdiction has to abide by its data-related laws (even if the company transfers data abroad), and each country's domestic data governance needs to be global in scope and interoperable in practice given the globally distributed nature of the Internet.

The focus for policymakers is ensuring they hold firms accountable regardless of where the firms store, process, or transfer data.

First, policymakers should focus on ensuring their legal frameworks make clear that firms with a legal nexus in their jurisdiction are responsible for managing data in a certain way, wherever the data is transferred and stored. This expectation could be made clear in law by declaring that companies doing business in a country are legally responsible for any failures to manage data (such as personal data) from that country, regardless of whether those failures are the fault of the firm in that country or abroad, or an affiliate or business partner in that country or abroad. In other words, a country's data-protection rules would travel with the data. Companies doing business in a given country would have a strong incentive to assist their business partners outside that country in adhering to its privacy protections, because its citizens and the government could seek remedies from that company for any privacy violations, such as a data breach, irrespective of whether that company or its partners were at fault.

Focusing on this key legal nexus concept would cover the behavior of many firms that attract regulatory scrutiny. Just as a global bank or manufacturer with branches or plants in a given nation is subject to that nation's privacy and security laws and regulations, foreign technology (or any other) firms cannot escape from complying with that nation's laws by transferring data overseas. But what about companies without legal nexus in a particular country (i.e., the firm has no physical presence, business activity, or marketing directed toward a specific foreign country)? For example, the citizens of nation A might visit the website of a small company located in nation B, which has different privacy and security laws. This company did not have a legal nexus in country A, so it cannot be expected to abide by the laws there. In this case, the only way nation A's laws can be enforced—whether or not they require data localization—is if they simply cut off their citizens' access to all foreign websites. This is not the case for most businesses involved in foreign digital activity, as they have legal nexus, but it highlights the fallacy of countries trying to enact policies that cannot be contained in-country, but affect the entire Internet.

This accountability-based approach is shared by most nations, after all, including for data privacy. For example, although the United States does not have an "adequacy" standard such as in the EU, the majority of companies in the United States must disclose certain data-privacy practices and adhere to those requirements, even when processing data outside the country, as they remain responsible for the data regardless of where it is processed. U.S. companies mitigate these risks by stipulating requirements in relevant data-handling and processing contracts they implement with other companies. For example, foreign companies operating in the United States must comply with the privacy provisions of the Health Insurance Portability and Accountability Act (HIPAA), which regulates U.S. citizens' privacy rights for health data—even if they move data outside the United States. And, if a foreign company's affiliates overseas violate HIPAA, then U.S. regulators can bring legal action against the foreign company's operations in the United States. In a way, such an approach are part of how firms already comply with data-related laws and regulations, as well as being a key part of existing data-transfer mechanisms countries and firms use (such as model contracts, binding corporate rules, the EU-US Privacy Shield, and the Asia Pacific Economic Cooperation's Cross-Border Privacy Rules (CBPR)).[9]

Policymakers need to focus on an accountability-based approach rather than mistakenly believing that forcing firms to exclusively store data locally (a concept known as "data localization") is the only way to enforce data-handling requirements on foreign organizations. While any country can demand extraterritorial application of its laws, it may not always be able to enforce them (as this can be quite complex). Multiple criteria are used by courts to determine when a country has the authority to impose its laws on those outside of its borders.[10] However, as long as a firm has a legal nexus within a country's jurisdiction, it has to abide by the laws of that country, regardless of where they store data. Just as international financial firms operating in a foreign country fall under the purview of that country's local regulatory agencies, regardless of where they transfer money to, so do firms that collect and use data as part of their business within that region. For example, many businesses have foreign workers (e.g., sales teams) or foreign assets (e.g., real estate, products, or bank accounts) that give foreign countries viable mechanisms for enforcement of

failures to abide by civil or criminal laws. Policymakers have leverage over firms doing business virtually because they can block access to domestic markets, such as by prohibiting local advertising.

Second, this accountability principle is based on the fact that modern technology, especially the Internet and cloud data storage, means that each country's domestic regulatory regime for data (such as for privacy) needs to be globally interoperable given that each country faces the same challenge in applying its laws to firms that may transfer data between jurisdictions. Interoperable privacy frameworks are the international extension of this accountability-based approach such that data is still able to flow between different privacy regimes, and countries'' data protection rules flow with it. The goal for interoperability also reflects the fact that there will be no one globally harmonized privacy regime. It is no surprise that interoperability—not harmonization or even adequacy—is a key objective of several of the leading data-protection initiatives, such as those from the Organization for Economic Cooperation and Development and Asia-Pacific Economic Cooperation (APEC).

No doubt, domestic regulators need the support and resources to fully operationalize such a framework in order to give them greater confidence in their ability to enforce local laws in the Internet era. In part, this can be done through additional international mechanisms that support the development and application of shared principles and cooperation between regulatory authorities. For example, there is obviously room for improvement in facilitating greater cooperation between different countries' privacy regulators. One example is the Global Privacy Enforcement Network, which was launched in 2010 by the privacy authorities of 12 countries, including the United States, Australia, Canada, France, Germany, and the United Kingdom.[11] Another is the APEC Cross-border Privacy Enforcement Arrangement (CPEA), which creates a regional framework for information sharing and cooperation on enforcement among privacy regulators.[12] At the next level below this, privacy regulators can set up bilateral arrangements (e.g., memorandums of understanding) with counterparts. Countries can then use these and bilateral mechanisms to both share information and best practices, and cooperate on joint investigations, such as what the U.S. Federal Trade Commission has done with over a dozen countries.[13]

The 2015 data breach at Ashley Madison (an adult dating website) highlights how privacy regulators can use these interoperability mechanisms to work together. Ashley Madison is headquartered in Canada, but its websites have a global reach, with users in 50 countries, including Australia. Although the firm that owns Ashley Madison does not have a physical presence in Australia, it conducts marketing in Australia, targets its services to Australian residents, and collects information from citizens in Australia. It therefore falls under Australian law. Canada's privacy regulator (the Office of the Privacy Commissioner of Canada) initiated a joint investigation with its Australian counterpart (the Office of the Australian Information Commissioner) based on each nation's respective participation in the APEC CPEA—which allowed for cooperation and the exchange of information on certain aspects of the investigation, despite each side conducting their own investigation according to their respective data privacy laws. The final analysis was that Ashley Madison held significant amounts of personal data (much of it sensitive) and should have had

security measures in place, such as an explicit risk-management process to identify information security risks. Ashley Madison agreed to a compliance and enforcement undertaking with both the Australian and Canadian privacy regulators to implement the regulators' recommendations.[14] Australia, Singapore, Japan, the United States and other leading digital economies need to articulate and enact a framework that is based on local accountability and interoperability in order to provide a clearer, and better, alternative to the two other main, contrasting approaches: efforts by countries (mainly European) to make other countries adopt their (universalist) approach to data privacy in order to make them responsible for enforcement (instead of holding firms responsible) and countries forcing firms to only store data locally (data localization). Essentially, the likely alternative to an approach based on accountability and interoperability is one characterized by Balkanization, as countries and subgroups of countries (in the case of the EU) enact artificial barriers that prohibit all or certain types of data flows.

Importantly, while the EU's data protection rules have gained some global traction over the past year, there is no reason to suspect that in the future another country or region might not put forth competing rules. For example, imagine if China created its own set of data protection rules and declared that any country wanting to do business in China must have identical data protection laws. Such a scenario would potentially force countries to choose one privacy regime or another. Therefore, it is unrealistic and impractical to demand universal rules on privacy. A better option would be to create an interoperable system.

An interoperable system would focus on "global protections through local accountability." The principle idea is that a country can enforce its rules on any foreign or domestic organization with legal nexus. Moreover, a country can enforce its rules on these organizations based on how they handle the data they collect, even if that data handling occurs abroad or with a third party. It is only through rigorous local enforcement that they are able to protect data globally. And it is this local enforcement that avoids the need to demand that all other countries abide by the same set of rules or pursue data localization policies.

Leading digital economies need to provide a clearer, better alternative to efforts by (mainly European) countries to make others adopt their approach to data privacy, and countries forcing firms to only store data locally.

Interoperability arises naturally from this framework, but countries can go further. In many cases, countries do share common rules, so there are opportunities to harmonize rules to make compliance easier. Moreover, countries can improve lawful government access to data stored through reciprocal agreements that streamline access among countries with similar legal protections, including through modernized mutual legal assistance treaties. Lastly, and perhaps most importantly, countries can expand their enforcement capabilities by entering into cooperative agreements that allow foreign regulators to investigate jointly, share findings, and impose penalties on violators, thereby strengthening the hands of regulators globally.

Beyond interoperability, the two alternative approaches to data governance data localization and the European Union's General Data Protection Regulation (GDPR)are problematic in their own ways. The EU's GDPR regime is problematic because it pushes for harmonization and tries to make foreign countries responsible for enforcing European data privacy standards instead of using domestic regulations to hold companies responsible for breaches of European data privacy laws. GDPR imposes a general prohibition on transfers of EU personal data to only a small group of foreign countries it has determined (as part of an opaque and ad hoc process) provide an "adequate" level of protection equal to data protection at home. A critical flaw in the European Union's approach is the mistaken logic that this country-by-country assessment approach is effective in promoting better data privacy and protection by companies that manage personal data.[15]

Furthermore, the EU's top-down approach is ultimately untenable, as differences in social, cultural, and political values, norms, and institutions are behind countries not regulating privacy the same way. For example, given the country's approach to data protection and privacy, it is inconceivable China would ever be deemed "adequate" from a European perspective. Yet, the fact that Europe has not applied to China the same standards it applies to the United States with regard to EU personal data highlights the arbitrary nature of its approach.[16] Ultimately, an interoperable framework for global protections through local accountability represents a more realistic and tenable approach to global data privacy—as, so far, outside European and British territories, only six countries have received a national adequacy finding from the EU: Argentina, Uruguay, Israel, Japan, New Zealand, and Canada.

In contrast, many U.S. firms rely on the EU-US Privacy Shield Framework (as the United states is not deemed adequate by the EU) to manage cross-border transfers of personal data with Europe, while a much smaller number of U.S. firms use APEC's CBPR for transfers to relevant APEC member economies. A 2017 International Association of Privacy Professionals-EY Annual Privacy Governance Report, in a survey of nearly 600 privacy professionals around the world, showed the importance of cross-border transfers of personal data and these two mechanisms. Overall, 55 percent of survey respondents' firms transferred personal data from the EU to the United States. Breaking this down, the survey showed how different firms rely on such flows and the EU-US Privacy Shield: 79 percent of EU and European firms, and 52 percent of U.S. firms; 82 percent of large multinationals with over $25 billion in revenue, and 34 percent of firms with under 5,000 employees; 73 percent of firms with a mature privacy practice, and 53 percent of early firms (along a of maturity curve of early, middle stage, and mature).[17] Meanwhile, 84 percent of respondents stated they will apply for CBPR sometime within the next few years.[18]

Data localization is becoming more common as a growing number of countries mistakenly believe it makes data more private and secure and is necessary to ensure regulatory oversight.

Meanwhile, data localization is becoming more common as a growing number of countries are forcing firms to store data locally in the mistaken belief that data is more private and secure when it is stored within a country's borders (not true) and needs to be stored locally to ensure regulatory oversight for data-related issues (also not true, as detailed in the subsequent section).[19] As to the former, controlling where organizations store data does not impact how they collect and use it (privacy)—or how they store and transmit it (security). Policies that lead to local data storage can actually undermine personal data protection, as without an independent judiciary and set of legal protections, governments can bring more pressure and tools to bear in forcing local providers to disclose data (for both social and political purposes). Even if a data privacy framework only requires a copy of data to be stored locally, rather than prohibiting transfers of all data, it nevertheless lays the groundwork for such an outcome. Furthermore, wherever data privacy intersects with cybersecurity, forced local data storage can make personal data more susceptible to inadvertent disclosures (i.e., data breaches) if the local data center is not committed to enacting best-in-class cybersecurity measures. Such inadvertent disclosures are the result of security failures. When it comes to data storage and protection, it is important the company involved (which either runs its own networks or uses a third-party cloud provider) be dedicated to implementing the most advanced methods to prevent such disclosures. The location of these systems has no bearing on the security of data.

Financial and Securities Regulators Should Focus on Firms Providing Access to Data (Not Where Data is Stored)

A growing number of countries, including China, India, Indonesia, Russia, and Turkey are enacting data localization requirements as part of financial oversight frameworks.[20.] At one stage, the United States pursued trade policy provisions that created the potential for localization, but it has since revised its approach. id="_ednref21">[21.] While many countries (such as India and Russia)use regulatory concerns as cover for protectionist intentions, there are other cases where underlying regulatory concerns over access to data are legitimate, albeit mistaken, and used to justify data localization. As policymakers discuss global digital economic issues, financial data also deserves attention, as it is among the most commonly targeted data categories (besides personal data).

Policymakers are enacting data localization requirements in the mistaken belief that it is the best and only way for data to remain accessible to government agencies for regulatory oversight. Policymakers are mistaken to believe firms can avoid oversight (and requests for data) by simply transferring data out of a given country. This is especially true for financial firms and firms listed on a local stock exchange, as they already have a clear legal nexus in a jurisdiction and have likely had to seek regulatory approval from local financial authorities to operate in a given jurisdiction. Indicative of many issues involving data, there are likely to be cases wherein jurisdictions come into conflict over access to data due to local laws and regulations (such as privacy). But similar concerns over other financial oversight issues have not prevented a more integrated global financial system. Nor should they, in the case of data governance. In contrast

they have led to the International Monetary Fund, the Financial Stability Board, and others working together on such shared concerns, including on data, as they recognize the mutual benefits of cooperation.

Policymakers should apply an accountability-based approach in ensuring firms provide timely access to data in response to requests for data from financial regulatory authorities (in the case of financial and payment services firms) and stock exchange administrators (for publicly listed companies). Modern cloud computing, which allows transfers of data with the mere click of a button, enables firms to provide timely access as part of regulatory oversight, while still allowing them to move financial data freely in order to provide secure, innovative, global services. Given the clear legal nexus of these firms, regulators should be confident they can ensure firms comply with data requests, regardless of where those firms store data. The focus for a nation's data governance frameworks should be on regulatory access to firms' data being timely, direct, and complete, regardless of where this data is stored. Obviously, if firms are unable to provide authorities with timely access to data, they should face legal penalties. But again, the focus should be on holding firms accountable regardless of where they store data. In this way, just as consumer safety and other laws apply to tangible goods that flow in and out of a country as part of international trade, regulatory, cybersecurity, and other rules should apply to both data and the financial firms that move and store data in other nations.

The respective approaches of the United States and the European Commission (EC) provide examples for other countries in regards to regulatory oversight and access to data. As part of efforts to build a Digital Single Market, EC is working to remove barriers to the transfer of company, tax, bookkeeping, and financial data, and asking that member states focus on mandating access.[22] For example, in 2015, Denmark changed its local data storage requirement for accounting data such that companies could store their data anywhere, as long as Danish authorities were given easy access to it on request.[23] This is where the focus should be: putting in place the legal framework to ensure companies can provide data to regulatory authorities in a timely manner.

Meanwhile, U.S. financial regulators recently enacted a data governance framework that focuses on access to data. U.S. regulators' initial concerns based on issues they had getting access to data in key banks' (such as Lehman Brothers') IT systems during the global financial crisis.[24] This made it difficult during bankruptcy proceedings for the regulators to access the data needed to unwind positions and ascertain what money was owed to whom.[25] However, subsequent legal reforms in the United States (e.g., the Dodd-Frank Act, enacted in 2010) have addressed these concerns by focusing on how companies disclose to regulators the way they manage their IT and data as part of regular prudential compliance activities. In the event of a crisis, regulators know companies will be able to provide the data they want.[26] These new mechanisms ensure regulators know how U.S. firms manage and secure their IT systems and how they store, access, and manage data on an ongoing basis (as part of periodic compliance activities).[27]

U.S. trade policy complements this domestic data governance framework with detailed, access-focused provisions that make data localization truly a last resort. Initially, the United States

created a loophole in the Trans-Pacific Partnership trade agreement for data localization by excluding financial data from the agreement's prohibitions on data transfer restrictions and not specifying (in detail) the exact interests and emergency scenarios in which this would be acceptable.[28] Recognizing this risk, the United States revised its approach in the U.S.-Mexico-Canada Agreement (USMCA) on trade to show how legitimate issues raised by cross-border data flows can be addressed while allowing the free flow of data as the default and predominant policy approach. It is important to note that the USMCA still treats financial services data differently (which in an ideal world, it would not), as neither the provisions that prohibit data localization nor data flow provisions apply to financial services. USMCA parties agreed to recognize "that immediate, direct, complete, and ongoing access by a Party's financial regulatory authorities to information of covered persons, including information underlying the transactions and operations of such persons, is critical to financial regulation and supervision, and recognize the need to eliminate any potential limitations on that access."[29]

Each member of the USMCA also agreed to provide financial firms with a reasonable opportunity to make changes to their IT systems (i.e., shift data storage from one jurisdiction to another) if they find they are unable to provide regulators with immediate and ongoing access to data. Highlighting (again) the central focus on access to data, the USMCA details that whenever a financial regulator requires a firm to change where it stores data, that new location does not necessarily have to be the firm's computing facilities in its home country, and may instead be a third-country jurisdiction where both the firm and its domestic regulators are confident they would have access. In designing these and other provisions, the United States Trade Representative's Office designed narrow and detailed language that facilitates government access to data for regulatory purposes, while ensuring countries remain committed to not enacting policies that require data localization or other barriers to data flows.[30]

Principle 2: Countries Should Put in Place New or Updated Mechanisms to Manage Cross-Border Access to Data for Law Enforcement Purposes

From a law enforcement perspective, the implicit expectation within this framework for data free flow with trust is that they are happy to allow data to flow freely as long as they have a clear and efficient legal framework with other countries that facilitates their timely access to data (related to a legitimate investigation) stored in that jurisdiction. The problem is existing legal processes and treaties (such as MLATs) are woefully out of date, needlessly complex, and often delayed due to poorly resourced local agencies. Countries have mismatched legal assistance treaties, conflicting laws, and differing norms. Indeed, there is currently no comprehensive framework for how to successfully navigate cross-border jurisdictional disputes, especially those involving the digital economy. As the threat of cybercrime rises, there is an increasing need for clarity on these questions, particularly regarding government access to data outside of its borders.

Existing legal processes and treaties (such as MLATs) are woefully out of date, needlessly complex, and often delayed due to poorly resourced local agencies.

If we are to establish a widely shared regime of free flow of data with trust, one key component needs to be that national law enforcement agencies trust they can get access to domestic data stored in other nations. This section outlines how leading countries should both push for new mechanisms (such as Cloud Act "executive agreements" and a Geneva Convention on the Status of Data), while also working to improve the existing mechanisms (such as MLAT 2.0 agreements) many countries rely upon.

Develop New Mechanisms to Address Legitimate Law Enforcement Concerns

The challenge facing Japan, the United States, and other likeminded countries that value international cooperation and the broader benefits of data flows is working together to establish new and improved international legal standards and mechanisms for facilitating legitimate law enforcement requests for cross-border access to data.[31.] The alternative some countries are pursuing under the guise of law enforcement interestsdata localization—threatens to undermine the global digital economy, especially if such an approach becomes the norm, as it would raise the specter of many—or perhaps even all—countries being stymied in their pursuit of cross-border criminal investigations (as each country would horde data locally). It would be better for countries to recognize the mutual benefit in implementing new and better mechanisms to help each other, given the increasing frequency in which local authorities encounter investigations that involve data held in another jurisdiction.

Ideally, countries would come together to negotiate a new multilateral agreementa Geneva Convention on the Status of Datato establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of international law enforcement requests, and limit unnecessary government access to data on citizens of other countries.[32] This would also help countries follow similar rules and procedures for cross-border law enforcement requests and actions.[33] And it would address the issues of localization and barriers to data flows, with parties agreeing not to enact data localization (as this would undermine the central point of the agreement).

Such a multilateral initiative would be based on national sovereignty, as different nations have different sets of values, priorities, and legal systems. And because Internet companies offer services over global networks, it is often the case that two or more countries have interests in the same data. This initiative should not force a particular nation's policies, such as promoting the strict standard of probable cause to gather evidence (as in the case of the United States) or allowing government access to evidence at the detriment of personal freedoms (as in the case of nations such as China and Russia), on the rest of the world. Therefore, each business should be subject to the laws of each country in which they have a legal presence. This principle would

ensure no company can escape complying with a nation's laws by simply transferring data overseas. It is simply a matter of coming up with a framework to create interoperability between different countries' approaches.

Ideally, countries would come together to negotiate a new multilateral agreementa Geneva Convention on the Status of Datato establish international rules for transparency, settle questions of jurisdiction, engender cooperation for better coordination of law enforcement requests, and limit unnecessary government access to data on citizens of other countries.

The United States' experience with the Cloud Act provides an example of the types of law enforcement cases that can arise in today's global digital economy, and how policymakers should respond in creating new mechanisms to facilitate cross-border law enforcement requests for data. The Cloud Act stemmed from a case in late 2013 when U.S. federal law enforcement officials obtained a warrant as part of an anti-narcotics investigation to seize the contents of an email account belonging to a Microsoft customer whose data the company stored in Dublin, Ireland.[34] Microsoft refused to comply with the order, arguing that the U.S. government cannot force a private party to do what U.S. law enforcement has no authority to do itself: use a warrant to conduct a search-and-seizure operation on foreign soil. This case exposed the cracks in the foundation of the current framework used by law enforcement agencies to access digital information and determine jurisdiction on the Internet.

In response, U.S. policymakers enacted the Cloud Act to reform the current system and address the problems the Microsoft case raised, while protecting consumer privacy, enhancing the capabilities of law enforcement, and preserving international comity. The legislation authorizes the U.S. government to form reciprocal data-sharing agreements (called "executive agreements") with other countries, giving them an incentive to remove barriers to sharing data with U.S. law enforcement. It also creates a statutory right for companies to challenge data requests from law enforcement that conflict with other nations' laws.[35]

Importantly, the Cloud Act also requires the U.S Department of Justice (DOJ) to provide a written certification that a country (with whom it enters an executive agreement) "demonstrates a commitment to promote and protect the global free flow of information and the open, distributed, and interconnected nature of the Internet."[36] Even though the ability to make such a certification is one of many factors DOJ must consider when entering into an agreement with another country, a requirement to localize data suggests DOJ would consider this as a contravention of the CLOUD Act's criteria. The United States has reportedly begun negotiations on executive agreements with the United Kingdom, and reportedly plans to use this agreement with the United Kingdom as a template in negotiations with other countries and regions, including the European Union, Australia,

and New Zealand.[37] In a similar fashion, the European Union's e-evidence initiative aims to create a legal framework to enable judicial orders to be addressed directly to service providers based in other member states.[38]

Update Existing MLAT Agreements

Beyond the U.S. Cloud Act and EU e-evidence reforms, countries should also improve existing processes and tools used to manage cross-border law enforcement requests for data, especially MLATs, as they are commonly used around the world. In this way, countries can put in place the individual building blocks that support the longer-term goal of a new multilateral agreement. To encourage more countries to adopt new or updated MLATs with each other, leading countries should also standardize and strengthen these agreements. The U.S. government should work with major economic organizations and forums, such as the European Union, the Organization of American States, and APEC, to establish and adopt model MLAT language, or a "MLAT 2.0." This treaty should create a common process so that governments do not necessarily need to negotiate agreements with each individual country, but instead, allows them to use fairly standardized agreements across many nations. The goals of an MLAT 2.0 would be fourfold.

First, MLAT 2.0 should create a common framework for when and how countries may use domestic authorizations to access data outside their borders. This may include arrangements such as reciprocal recognition of domestic search warrants (when countries meet certain legal standards) in order to expedite the process. Similarly, the agreement may include comity analyses or notice requirements as a condition of this reciprocal recognition.

Second, MLAT 2.0 should commit countries to modernizing their methods for responding to foreign data requests, such as through the processes outlined in the previous recommendation. Third, countries should commit to complying with their counterparts' lawful requests for data in a timely fashion, unless those requests would violate mutually agreed upon provisions, such as for national security reasons. Fourth, countries should report the number of requests they receive, the number of requests they fulfill, response times, and progress in their modernization efforts. The goal of reporting is to hold participating nations publicly accountable for their timeliness in adopting and modernizing MLAT processes, as well as to identify inefficiencies in the process.

Once adopted, each country should push their trading partners to use this MLAT 2.0 (given the trade implications of data localization), thereby encouraging more countries to adopt improved MLATs with one another. The United States should lead by example and work in good faith to update its MLATs to fit this model, and establish new MLATs with countries where no treaty currently exists. Working in tandem with its approach to cross-border law enforcement requests, the United States and its likeminded partners, as well as various regional economic forums, can streamline and expand the number of countries fielding MLATs.

Strengthen Domestic MLAT Processes to Support Updated MLAT Agreements

Japan, the United States, and likeminded countries should ensure the relevant domestic

institutions that manage foreign governments' requests for data are efficient and well-funded. Streamlining the processes, including reducing the time it takes for domestic law enforcement to respond to foreign counterparts, would help alleviate concerns some policymakers have regarding cross-border data storage, as it weakens the incentives for data localization.

The United States presents a clear case where improvements have already been made, but more are required. Since 2000, the number of requests from foreign authorities handled by DOJ has increased nearly 85 percent.[39] A 2013 report in which several U.S. officials were interviewed concluded that electronic evidence transfers are the most resource-intensive demands on DOJ's Office of International Affairs.[40] In 2015, DOJ requested $24 million be added to its budget to hire additional personnel to handle MLAT requests and train foreign law enforcement officials on how to meet U.S. evidentiary standards for MLAT requests.[41] The request also sought to expand MLAT responsibilities to the Federal Bureau of Investigation by creating a dedicated unit that manages intake and tracking of MLAT requests.[42] In 2017, DOJ requested $10 million for the same purposes, including the hiring of 97 positions related to MLAT reform.[43] The U.S. Congress should give DOJ the funding it needs to modernize how it responds to foreign MLAT requests. In addition to funding, Congress should direct DOJ to review and streamline the process it uses to fulfill foreign MLAT requests. The 114th Congress considered several pieces of legislation that would improve the effectiveness and efficiency of this process.[44]

Leading Countries Should Use Reform Efforts and Revised Mechanisms to Push Back Against Foreign Data Localization Requirements and Data Havens

Countries that adopt MLAT 2.0 agreements, Cloud Act executive agreements, or any other similar agreements should pledge not to impose data localization restrictions on companies for law enforcement purposes. Including anti-localization provisions in new agreements makes sure parties to those agreements do not have it both ways—in terms of having an executive agreement with the United States and other countries to facilitate more efficient access to data in their jurisdictions, while also forcing firms to store data locally to facilitate government access. Including this explicit provision would create a situation whereby there would be no benefit to data localization when it comes to law enforcement access to data.

There is a mutual benefit in combining updated MLAT agreements and processes with a pledge to avoid data localization, as the alternative (widespread data localization) would inevitably reach a tipping point whereby enough countries doing it would make cross-border cooperation on law enforcement investigations that much harder for everyone. Indeed, some policymakers already see limiting foreign investigations as a justification for enacting data localization policies.[45]

There is a mutual benefit in combining updated MLAT agreements and processes with a pledge to avoid data localization, as the alternative would inevitably reach a tipping point.

As countries sign up to the Geneva Convention on the Status of Data, and this network of new Cloud Act executive agreements and MLATs emerges, responsible member countries should would be better placed to identify those countries that act in bad faith in attempting to circumvent good faith efforts and international legal processes for providing law enforcement agencies lawful access to data as "data havens." Under these respective agreements, nations would (ideally) also have the authority to block data flows to, or ban companies from basing servers in, these scofflaw data havens, as they have demonstrated they cannot be trusted to work with their counterparts on shared interests in the global digital economy, such as cross-border law enforcement investigations.

Principle 3: Countries Should (Responsibly) Stop Data Flows of Illegal Content

Some people interpret the concept of free flow of data across borders to mean all data should be allowed to traverse borders without barriers. But within the concept of data free flow with trust, it is important to recognize that not all data flows should be treated the same, as some data flows are rightly illegal. Thus, there is nothing contradictory about strongly supporting the global free flow of data while also supporting the blockage of the flow of illegal data, any more than it is to strongly support the free trade of goods, while supporting the blocking of trade in endangered species or human trafficking.

While policymakers can obviously put in place domestic laws to manage illegal online activity within their own country, due to the globally distributed nature of the Internet, such activity often remains accessible from foreign providers. From a pragmatic perspective, this is why a growing number of countries ask their Internet service providers (ISPs) to block access to websites engaged in illegal activities—such as those facilitating cybercrime, child pornography, or terrorism—because it is one of the few means available to authorities responding to illegal services and materials hosted abroad. Blocking websites engaged in intentional and systematic copyright infringement should not be considered any different. Obviously, it is important that any such framework be transparent and include legal checks and balances to ensure it is used appropriately, but its growing use around the world shows that this is eminently achievable and that website blocking can be an effective part of a country's policy tool box to promote and protect creativity and innovation in the global digital economy.[46]

Within the concept of data free flow with trust, it is important to recognize that not all data flows should be treated the same, as some are rightly illegal.

Many countries use website blocking to apply both new and existing legislation to a range of legitimate public policy goals that involve the Internet.

Examples of the types of websites countries block include:

- child pornography (many countries);
- malware (e.g., Australia);[47]
- investment fraud (e.g., Australia);[48]
- online gambling (e.g., Quebec, Canada and Singapore);[49]
- pornography (e.g., India);[50]
- prostitution (e.g., India);[51]
- terrorism (e.g., the United Kingdom, Australia, France, and India);[52] and
- copyright-infringing content (at least 42 nations).[53]

As an example, website blocking is used extensively to block child pornography websites. The 190 members of the International Criminal Police Organization (INTERPOL) voted unanimously to promote the use of all technical tools, including website blocking, to fight child pornography. INTERPOL maintains a list of domains containing websites that disseminate the most severe child abuse material worldwide as part of a "worst of" list.[54] It also provides domains, not URLs, for blocking. As INTERPOL explains, blocking does not by itself remove the offending content, but it does dramatically reduce the amount that is accessible and available to most users. As with many other issues, website blocking is used in conjunction with other measures.

The world's leading digital economies should recognize that website blocking is a constructive intellectual property (IP) policy tool for copyright enforcement and to enact changes that allow website blocking, if they do not already allow it (as Australia, Singapore, and the United Kingdom do). Such formal recognition would reflect the fact that website blocking for copyright infringement has finally been normalized as an anti-piracy tool around the world. For online copyright infringement, there are at least 42 countries that have either adopted and implemented, or are legally obligated to adopt, measures ensuring ISPs block access to copyright-infringing websites, as figure 2 shows.[55] The first website blocked for copyright infringement was AllofMP3 in Denmark in 2006. In the decade thereafter, fewer than 1,000 websites were blocked. However, over the past three years, countries have blocked more than 3,000 new piracy websites.[56] The actual figure

is likely much higher, as some countries, such as the United Kingdom, do not release specific details on which websites are being blocked, so as not to alert website operators. In February 2019, a Motion Picture Association of America presentation outlined that countries block a total of 3,966 websites and 8,150 domain names. Europe is home to the most countries that allow website blocking. Portugal and Italy have each blocked 944 and 855 websites respectively.[57] Furthermore, some countries, such as India, Singapore, and the United Kingdom, now allow "dynamic" blocking orders that extend to proxy websites that piracy operators create after their primary sites are blocked, and are to be enacted during live sporting events.[58] Some of the lessons to take away from the growing use of website blocking is that for it to be effective and workable, it needs to be predictable, transparent, accountable, low-cost, and quick to implement. If countries enact a framework along these lines, it can be a reasonable and useful tool to reduce piracy and encourage consumption of legal content.

Figure 2: Countries that allow website blocking for copyright infringing content [59]

Argentina, Australia, Austria, Belgium, Bulgaria, Croatia, Czech Republic, Cyprus, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, India, Indonesia, Ireland, Israel, Italy, Korea, Latvia, Liechtenstein, Lithuania, Luxembourg, Malaysia, Malta, Mexico, Netherlands, Norway, Poland, Portugal, Romania, Russia, Singapore, Slovakia, Slovenia, Spain, Sweden, Thailand, and the United Kingdom.

Website blocking is a logical weapon to use given all the targets and tools countries have to fight digital piracy. Domestically, the first of these is straightforward and already well underway: enacting policies that support an increase to the number of legal service providers in order to make it easier and cheaper for users to get legal media content online instead of using piracy sites. Alongside this, countries can enact legal remedies to combat certain activities. For example, for domestically hosted content in the United States, copyright holders rely on remedies in the Digital Millennium Copyright Act, which has a "notice and takedown" process for rights holders to

get website operators to remove infringing material. Domestic stakeholders, such as brand owners, advertising intermediaries, and rightsholders, can also work together to voluntarily address aspects of the digital piracy ecosystem, such as by ensuring ads from reputable brands are not placed on piracy websites (thus cutting off a source of income).[60]

Fighting digital piracy gets much harder at the international level. The first option is for law enforcement agencies to specifically target website owners who operate digital piracy sites.[61] However, in most cases, law enforcement cannot get cooperation from their counterparts in other countries to remove infringing material. What this highlights is that many countries are home to digital piracy sites, as they have governments that will not or cannot shut them down, either because there are weak or nonexistent intellectual property protections or for political reasons. Despite the fact that virtually every nation that acts as a haven for pirate sites is a member of WTO and World Intellectual Property Organization (WIPO) and has signed on to multilateral agreements protecting intellectual property—such as the Trade-related Aspects of Intellectual Property Rights (TRIPS) agreement—many nations refuse to effectively address digital piracy in their own jurisdictions, such as is the case for Brazil, Pakistan, Russia, and Ukraine.[62] This weakens trust in these agreements. Thus, absent changes to these institutions, or a change in attitude of governments of scofflaw nations, governments will need to work with Internet intermediaries as the main solution.

Website blocking for piracy, child pornography, or other illegal material is never going to be the silver bullet in stopping the distribution or access to certain illicit material, but it can definitely play a role. While there may be ways for users and piracy site operators to circumvent these methods (such as the use of virtual private networks), it is important to remember the aim of website blocking, such as other online enforcement methods, is not to eliminate online piracy altogether, but to change consumers' behavior by raising the cost—in terms of time, risk, and willingness to find alternative sites and circumvention tools—in order to make the legal sources of content more appealing, thus supporting the creators and others that work to provide this material.

For example, an April 2016 Carnegie Mellon University study shows that website blocking in the United Kingdom has been effective in fighting digital piracy. The study used consumer data to analyze the impact of a court order for ISPs to block 53 websites in the United Kingdom in November 2014. It showed that website blocking, when done on a large-enough scale, can shift consumers from accessing copyright-infringing material to consuming legal content online.[63] The study proves an intuitive understanding about online copyright enforcement: If enough piracy sites are blocked, then people will shift to legal sources, especially given the growing number of such services.

Proposals to use website blocking often face a range of ideological opposition, especially that blocking is antithetical to efforts to preserve a "free and open" Internet. While this is a rightly and broadly supported goal, at least in most democratic nations, it does not mean every website should be freely accessible.[64] Just as supporting bans on the importation of ivory or cross-border human trafficking does not make one a protectionist, supporting website blocking for sites dedicated to piracy does not make one an opponent of a free and open Internet. Clearly, society should want as

little as possible to be blocked or taken off the Internet, and that such processes should have appropriate legal checks and balances. But this does not mean policymakers should oppose attempts to block online materials that are clearly illegal.

The second major criticism is website blocking will establish a negative precedent if used by democratic countries, and will weaken the moral authority of democratic nations to criticize totalitarian governments for limiting Internet access unrelated to intellectual property. Critics claim these governments would point to democratic nations' use of website blocking to justify their own Internet censorship. But there is no comparison between a country that uses detailed and transparent legal means, supported by an independent legal system, to administer and enforce intellectual property online and a country simply censoring political speech online. Likewise, the U.S. government has not abandoned laws requiring child pornography to be blocked because it thinks doing so would give carte blanche approval to dictatorships that want to block dissenting websites. Online intellectual property enforcement is far from alone in being a public policy that could be misused in order to pursue unrelated or illegitimate objectives. In each case, what matters is the actual intent and the integrity of the process involved in administrating these policies.

Principle 4: Countries Should Support (Not Undermine) Encryption's Role in Securing Data Flows

For data to flow "with trust," as specified by Prime Minister Abe, it needs to take into consideration the key technology people and businesses rely on to ensure the confidentiality of data: encryption.[65.] Encryption is a process that secures information from unauthorized access or use, mainly by changing information which can be read (plaintext) to make it so it cannot be read (cipher text).[66.] Over the last few decades, researchers and firms have steadily gotten significantly better at using encryption to secure the privacy and integrity of data—which has been integrated into goods and services in order to improve security for consumers and businesses. In particular, the development of public-key cryptography, which allows users to communicate securely over an untrusted network such as the Internet, has underpinned most modern ICT products and services. As such, encryption has become a fundamental component of improving cybersecurity, and law enforcement, civil society, security experts, and even the former president of the United States all agree on its benefits.[67.] As ITIF argued in "Unlocking Encryption: Information Security and the Rule of Law," the problem is that as the methods citizens and businesses use to secure their information have evolved, some governments, citing law enforcement and national security concerns, have pushed back and proposed or enacted laws that undermine encryption and the beneficial role it plays in today's economy.[68.]

For data to flow "with trust," as specified by Prime Minister Abe, it needs to take into consideration the key technology people and businesses rely on to ensure the confidentiality of data: encryption.

Encryption is increasingly important to the global digital economy, as it protects the confidentiality and security of data. Whether consumers realize it or not, encryption is as ubiquitous as the many ICT devices they use in their daily lives. Even without a user's interaction, devices may use encryption when communicating to other devices to ensure commands received from one device are authenticated before being executed.[69] As such, encryption allows consumers and firms to securely engage in a variety of online activities, such as through access to services (e.g., logons, passwords, e-commerce applications) and privacy of communications (e.g., email, instant messaging, virtual private networks). Businesses use encryption to ensure their research is kept confidential from competitors and hackers, and to ensure transactions with their suppliers and customers are authentic. Essentially, strong encryption helps firms and consumers securely communicate with systems and individuals around the world, thereby facilitating the transactions that allow the global digital economy to grow.[70]

Firms use encryption to ensure, and prove, compliance with laws and regulations that require they use "technical measures" to protect data, such as for privacy, financial, data security, and other issues. Such encryption-related provisions focus on the firms using technological tools to ensure they protect certain categories of data, while still preserving their ability to transfer, share, and use data. For example: HIPAA uses encryption to protect personal health information; encryption of cardholder data is an acceptable method of rendering data unreadable in order to meet the Payment Card Industry Data Security Standard, which is a set of security controls (an industry-required standard) businesses are required to implement to protect credit card data; and the European Union's GDPR emphasizes data governance and accountability when firms manage personal data, requiring them to assess the risk of data loss and data breach and commit them to consider technical "state of the art" measures to mitigate those risks, including encryption.[71]

Proposed and enacted government policies that undermine encryption have taken on a few forms:

- Requirements that firms license or register encryption with government agencies
- Firms only using a government-mandated encryption standard
- Local encryption key storage
- Prohibitions on client-side encryption
- Firms disclosing source code

- Legal and administrative requirements that firms provide vague, arbitrary, and nontransparent decryption or technical support to government agencies, including installing "back doors" into their products

Most recently, Australia, China, and the United Kingdom have enacted laws mandating tech firms cooperate with government to install back doors into ICT products and services.[72] The United States considered such laws, but decided against them. Likewise, both Germany and the Netherlands have publicly disavowed backdoors in encryption products.[73] Previous government efforts to limit encryption have had various levels of success in restricting wider use of secure technology, such as the much-maligned Clipper Chip proposal in the 1990s.[74] Other attempts have been clandestine, generating distrust among the general public, foreign governments, and industry stakeholders, such as the National Security Agency's surreptitious efforts to introduce backdoors into U.S. products and hide security vulnerabilities it has discovered in commercial systems in order for the government to exploit those weaknesses.[75]

Governments should not restrict or weaken encryption. Any government attempt to undermine encryption reduces the overall security of law-abiding citizens and businesses, makes it more difficult for companies from countries with weakened encryption to compete in global markets, and limits advancements in information security. For example, mandating companies build so-called back doors into their products to facilitate government access undermines the integrity of firms' encryption products. A weakness or opening provided for one stakeholder inevitably weakens the overall level of protection, as it provides an opening for others, such as hackers. Furthermore, such requirements raise a whole range of concerns for firms, such as defining technical requirements based only on a particular government's subjective view of what is reasonable and practical, without due regard for how encryption is developed, how it works, or how it is deployed globally.[76]

Moreover, attempts to restrict or weaken encryption would be ineffective at keeping this technology out of the hands of criminals and terrorists, who would be able to access encryption technology on their own.[77] Furthermore, such requirements do not even guarantee success. With data at rest (in electronic storage), even if a law enforcement agency gets a court order to access a person's data stored by a third-party provider (e.g., a cloud storage company), it would not be able to make sense of the data if it is encrypted and that agency does not have the key. If firms that provide the service to the person do not have the key to their customers' encrypted data, then they will be unable to comply with requests by intelligence agencies to search through this data. For data in motion (information moving between two or more endpoints), law enforcement may try to gain access through court-ordered wiretaps to monitor specific communications. Again, law enforcement may be able to gain access to messages passed through a messaging service, but if the communications are encrypted end-to-end so only the endpoints (users) have keys, law enforcement officials would be unable to decipher it.

While many governments have enacted (or considered) such policies for law enforcement and national security reasons, others have used these concerns as a disguise for mercantilism. Encryption products are often at the cutting edge of technological innovation, so some countries

view regulatory requirements as a way to help local firms catch up by providing copies or access to source code and related material. Similarly, some countries see regulatory restrictions as a way to discriminate against foreign firms and their products. For example, a requirement for a local encryption key storage would result in a firm or its customer having to set up a local server to facilitate the authentication and encryption process.

CONCLUSION

Just as aeronautical law evolved to support the expansion of global civil aviation, and international maritime law advanced to support the development of a global shipping industry, so too should countries and relevant stakeholders construct a framework to address issues raised by cross-border data flows. At the heart of this approach should be the recognition that data and data flows are beneficial, and that countries are most likely to come together around a pragmatic framework that addresses key shared issues that ensure firms are held accountable for how they manage data (wherever they store it) and helps people and firms maximize the social and economic benefits, while minimizing detrimental aspects (such as access to illegal content) and avoiding policies that undermine the confidentiality and security of data (such as through the use of encryption).

ENDNOTES

1. Shinzo Abe, "'Defeatism about Japan is now defeated': Read Abe's Davos speech in full," World Economic Forum, January 23, 2019, https://www.weforum.org/agenda/2019/01/abe-speech-transcript/.

2. Nick Wallace, "Europe Should Put Data at the Service of Society," *Euractiv*, October 14, 2016, https://www.euractiv.com/section/digital/opinion/europe-should-put-data-at-the-service-of-society/; Daniel Castro and Joshua New, "The Promise of Artificial Intelligence" (Center for Data Innovation, October 2016), http://www2.datainnovation.org/2016-promise-of-ai.pdf Alexander Kostura and Daniel Castro, "Europe Should Promote Data for Social Good" (Center for Data Innovation, October 3, 2016), http://www2.datainnovation.org/2016-data-social-good.pdf

3. For example, see: Nick Wallace and Daniel Castro, "The State of Data Innovation in the EU" (Center for Data Innovation, October 2017), http://www2.datainnovation.org/2017-data-innovation-eu.pdf; Daniel Castro and Travis Korte, "Data Innovation 101" (Center for Data Innovation, November 2013), https://www.datainnovation.org/2013/11/data-innovation-101/.

4. Daniel Castro, "A Declaration of the Interdependence of Cyberspace," *ComputerWorld*, February 8, 2013, https://www.computerworld.com/article/2494710/a-declaration-of-the-interdependence-of-cyberspace.html.

5. In effect, cyber-libertarians want one universal rule: no government-imposed rules" John Perry Barlow's "Declaration of Independence from Cyberspace" is the epitome of the cyber-libertarian philosophy, in which he states national governments have no authority on the Internet, and are unwelcome.

6. For further details see: Daniel Castro and Robert Atkinson, "Beyond Internet Universalism: A Framework for Addressing Cross-Border Internet Policy" (Information Technology and Innovation Foundation, September 2014), http://www2.itif.org/2014-crossborder-internet-policy.pdf.

7. Ibid.

8. See: "Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography" (United Nations, May 25, 2000), http://www.ohchr.org/EN/ProfessionalInterest/Pages/OPSCCRC.aspx.

9. For example, firms may implement (and demonstrate) accountability through various internal privacy and information management programs, regulated frameworks (such as the EU's Binding Corporate Rules and the EU-US Privacy Shield), industry codes of conduct, third-party certifications and seals, and international standards. Binding corporate rules state firms may transfer personal data across borders within a single company. See: "The Case for Accountability: How it Enables Effective Data Protection and Trust in the Digital Society" (Center for Information Policy Leadership, July 23, 2018), https://www.informationpolicycentre.com/uploads/5/7/1/0/57104281/cipl_accountability_paper_1_-_the_case_for_accountability_-_how_it_enables_effective_data_protection_and_trust_in_the_digital_society.pdf.

10. When determining whether a country has jurisdiction over an organization, factors such as physical presence, business activity, and marketing are likely to be considered.

11. International Consumer Protection and Enforcement Network website, https://www.icpen.org/; Global Privacy Enforcement Network website, https://www.privacyenforcement.net/

12. "APEC Cross-border Privacy Enforcement Arrangement (CPEA)," Asian-Pacific Economic Cooperation, https://www.apec.org/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group/Cross-border-Privacy-Enforcement-Arrangement.aspx.

13. Federal Trade Commission, International Competition and Consumer Protection Cooperation Agreements, https://www.ftc.gov/policy/international/international-cooperation-agreements.

14. The Office of the Privacy Commissioner of Canada (OPC), Joint investigation of Ashley Madison by the Privacy Commissioner of Canada and the Australian Privacy Commissioner/Acting Australian Information Commissioner (PIPEDA Report of Findings #2016-005), August 22, 2016, https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2016/pipeda-2016-005/.

15. See: Robert Atkinson, "Don't Just Fix Safe Harbor, Fix the Data Protection Regulation," *Euractiv,* December 18, 2015, https://www.euractiv.com/section/digital/opinion/don-t-just-fix-safe-harbour-fix-the-data-protection-regulation/.

16. For example, a report for the European Parliament on data protection in China states that there is "no common ground… found between two fundamentally different systems both in their wording and in their raison d'etre." The report takes a relativist approach by saying China's culture and approach to human rights means the European Union should treat China differently when it comes to trade and privacy issues, despite the fact that "China does not have a general data protection act but traces of data protection may be found in a multitude of sector-specific legal instruments." Paul de Hert and Vagelis Papakonstantinou, "The Data Protection Regime in China" (Brussels: report for the European Parliament's Policy Department for Citizens' Rights and Constitutional Affairs, October 2015), http://www.europarl.europa.eu/RegData/etudes/IDAN/2015/536472/IPOL_IDA(2015)536472_EN.pdf.

17. *IAPP-EY Annual Privacy Governance Report 2017* (International Association of Privacy Professionals), https://iapp.org/media/pdf/resource_center/IAPP-EY-Governance-Report-2017.pdf

18. Ibid.

19. Nigel Cory, "Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/cross-border-data-flows-where-are-barriers-and-what-do-they-cost

20. For details on cases in India and Turkey, see: Nigel Cory, "The Ten Worst Digital Protectionism and Innovation Mercantilist Policies of 2018" (Information Technology and Innovation Foundation, January 28, 2019), https://itif.org/publications/2019/01/28/ten-worst-digital-protectionism-and-innovation-mercantilist-policies-2018.

21. Ibid, 19; Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements"(Information Technology and Innovation Foundation, April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf; Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists"(Information Technology and Innovation Foundation, July 7, 2016), https://itif.org/publications/2016/07/07/tpp%E2%80%99s-financial-data-carve-out%E2%80%94ustr-closes-loophole-digital-protectionists.

22. Julia Fioretti, "EU looks to Remove National Barriers to Data Flows," *Reuters,* September 29, 2016, http://www.reuters.com/article/us-eu-data/eu-looks-to-remove-national-barriers-to-data-flows-idUSKCN11Z19Q

23. "Requirements for Exemption to Store Electronic Accounting Records Abroad Will Be Abolished," Horten website, accessed November 9, 2017, http://en.horten.dk/News/2015/February/Requirement-for-exemption-to-store-electronic-accounting-records-abroad-will-be-abolished

24. The ability of the U.S. Federal Reserve and Federal Deposit Insurance Corporation (FDIC) to use and analyze Lehman's IT system and data was reportedly hindered as the bank's network became fragmented, overseas subsidiaries were sold off, some IT systems in overseas subsidiaries were turned off, some key IT staff departed, and restrictions on data flows were imposed due to insolvency filings in other countries—as was the case when the United Kingdom's financial regulator took over Lehman Brothers' European division. Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements" (Information Technology and Innovation Foundation, April, 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf; Rosalind Wiggins and Andrew Metrick, "The Lehman Brothers Bankruptcy: The Effect of Lehman's U.S. Broker Dealer" (Yale Program on Financial Stability Case Study 2014-3E-V1), http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2588556; Administrative Office of the United States Courts, "Report Pursuant to Section 202(e) of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010" (Washington, D.C., July 2011); Lemieux, "Financial Records and Their Discontents"; "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009," PricewaterhouseCoopers, accessed April 4, 2016, http://www.pwc.co.uk/en_uk/uk/assets/pdf/lbie-progress-report-140409.pdf.

25. "Lehman Brothers International (Europe) in Administration: Joint Administrators' Progress Report for the Period 15 September 2008 to 14 March 2009."

26. The law outlined extensive new rules that require "systemically important financial institutions" (SIFIs) to prepare "resolution plans"—also known as "living wills"—that specify a company's strategy for "rapid and orderly resolution in the event of material financial distress or failure of the company. "Resolution Plans," Board of Governors of the Federal Reserve System, accessed April 4, 2016, https://www.federalreserve.gov/bankinforeg/resolution-plans.htm

27. These "living wills" are required to provide a broad range of information relevant to resolution planning and implementation including, for example, detailed descriptions of organizational structures, credit exposures and cross-guarantees, and supporting data. The relevant section on IT and data states, "Management Information Systems; Software Licenses; Intellectual Property. Provide a detailed inventory and description of the key management information systems and applications, including systems and applications for risk management, accounting, and financial and regulatory reporting, used by the covered insured depository institution (CIDI) and its subsidiaries. Identify the legal owner or licensor of the systems identified above; describe the use and function of the system or application, and provide a listing of service level agreements and any software and systems licenses or associated intellectual property related thereto. Identify and discuss any disaster recovery or other backup plans. Identify common or shared facilities and systems, as well as personnel necessary to operate such facilities and systems. Describe the capabilities of the CIDI's processes and systems to collect, maintain, and report the information and other data underlying the resolution plan to management of the CIDI and, upon request, to the FDIC. Describe any deficiencies, gaps, or weaknesses in such capabilities and the actions the CIDI intends to take to promptly address such deficiencies, gaps, or weaknesses, and the time frame for implementing such actions."

28. Nigel Cory, "The TPP's Financial Data Carve Out—USTR Closes a Loophole for Digital Protectionists"(Information Technology and Innovation Foundation, July 7, 2016), https://www.innovationfiles.org/the-tpps-financial-data-carve-out-ustr-closes-a-loophole-for-digital-protectionists/; Nigel Cory and Robert Atkinson, "Financial Data Does Not Need or

Deserve Special Treatment in Trade Agreements" (Information Technology and Innovation Foundation, April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf.

29. United States Trade Representative, "USMCA: Chapter 17: Financial Services," https://ustr.gov/sites/default/files/files/agreements/FTA/USMCA/Text/17_Financial_Services.pdf.

30. Nigel Cory and Stephen Ezell, "Comments to the U.S. International Trade Commission Regarding the United States-Mexico-Canada Agreement" (Information Technology and Innovation Foundation, December 17, 2018),https://itif.org/publications/2018/12/17/comments-us-international-trade-commission-regarding-united-states-mexico.

31. Daniel Castro, "The False Promise of Data Nationalism" (Information Technology and Innovation Foundation, December 2013), accessed June 29, 2017, http://www2.itif.org/2013-false-promise-datanationalism.pdf; Nigel Cory, "Cross-Border Data Flows: Where are the Barriers, and What Do They Cost?" (Information Technology and Innovation Foundation, May 1, 2017), https://itif.org/publications/2017/05/01/crossborder-data-flows-where-are-barriers-and-what-do-they-cost.

32. Alan McQuinn and Daniel Castro, "How Law Enforcement Should Access Data Across Borders" (Information Technology and Innovation Foundation, July 24, 2017), https://itif.org/publications/2017/07/24/itif-calls-united-states-lead-developing-new-approach-international-law.

33. For example, to address some of the issues raised here: "Data & Jurisdiction Work Plan" (The Internet & Jurisdiction Policy Network, February 28, 2018), https://www.internetjurisdiction.net/publications/paper/data-jurisdiction-work-plan

34. The user in the case enters in a "country code" at registration, which Microsoft uses to migrate that user's data to the closest data center, which is in Dublin, Ireland. At the time the warrant was issued, the U.S. government did not know where the data was stored. *Microsoft Corporation v. United States*, 15 F. Supp. 3d 466 (S.D.N.Y. 2014), Document Cloud, 3, http://www.documentcloud.org/documents/1149373-in-re-matter-of-warrant.html.

35. Information Technology and Innovation Foundation, "CLOUD Act Brings Congress Closer to Resolving Problem of Cross-Border Data Access, But Changes Needed to Avoid Jurisdictional Conflicts," news release, February 6, 2018, https://itif.org/publications/2018/02/06/cloud-act-brings-congress-closer-resolving-problem-cross-border-data-access.

36. Jonathan G. Cedarbaum, "Congress Enacts Law Clarifying Reach of Warrants for Overseas Data," *WilmerHale Blog*, March 28, 2018, https://www.wilmerhale.com/en/insights/blogs/wilmerhale-privacy-and-cybersecurity-law/congress-enacts-law-clarifying-reach-of-warrants-for-overseas-data; Owen Daugherty, "Cruz warns 'Space Force' needed to prevent space pirates," *The Hill*, May 15, 2019, https://thehill.com/opinion/cybersecurity/405422-will-the-us-capitalize-on-its-opportunity-to-stop-data-localization.

37. For example: Peter Swire and Justin Hemmings, "Recommendations for the Potential U.S.-U.K. Executive Agreement Under the Cloud Act," *Lawfare*, September 13, 2018, https://www.lawfareblog.com/recommendations-potential-us-uk-executive-agreement-under-cloud-act.

38. "Regulation on Cross Border Access to E-evidence: Council Agrees Its Position *sic.*," Council of the EU, July 12, 2018, https://www.consilium.europa.eu/en/press/press-releases/2018/12/07/regulation-on-cross-border-access-to-e-evidence-council-agrees-its-position/.

39. "Performance Budget, FY 2017 President's Budget" (Criminal Division, U.S. Department of Justice, 2017), accessed June 28, 2017, https://www.justice.gov/jmd/file/820926/download.

40. Ibid.

41. Department of Justice, "Attorney General Holder Announces President Obama's Budget Proposes $173 Million for Criminal Justice Reform," press release, March 4, 2015, accessed June 29, 2017, https://www.justice.gov/opa/pr/attorney-general-holder-announces-president-obama-s-budget-proposes-173-million-criminal

42. FY 2014 had no current FBI services for MLAT reform initiatives. The FY 2015 request had $3.2 million and 14 positions, including 7 agents, for these FBI efforts. "FY 2015 Budget Request—Mutual Legal Assistance Treaty Process Reform" (U.S. Department of Justice, 2014), accessed June 29, 2017, https://www.justice.gov/sites/default/files/jmd/legacy/2014/07/13/mut-legal-assist.pdf.

43. "FY 2017 Budget Request – National Security" (U.S. Department of Justice, 2016), accessed June 29, 2017, https://www.justice.gov/jmd/file/822376/download.

44. Congressman Tom Marino, "Reps. Marino, DelBene Introduce LEADS Act," press release, February 27, 2015, accessed June 29, 2017, https://marino.house.gov/media-center/press-releases/reps-marino-delbene-introduce-leads-act; Senator Orrin Hatch, "Hatch, Coons, and Heller Introduce Bipartisan LEADS Act to Protect Data Stored Abroad," press release, February 12, 2015, accessed June 29, 2017, https://www.hatch.senate.gov/public/index.cfm/2015/2/hatch-coons-and-heller-introduce-bipartisan-leads-act-to-protect-data-stored-abroad; Senator Orrin Hatch, "Hatch, Coons, Heller Introduce Bipartisan International Communications Privacy Act," press release, May 25, 2016,, accessed June 29, 2017, https://www.hatch.senate.gov/public/index.cfm/2016/5/hatch-coons-heller-introduce-bipartisan-international-communications-privacy-act.

45. Daniel Castro and Alan McQuinn, "Beyond the USA Freedom Act: How U.S. Surveillance Still Subverts U.S. Competitiveness" (Information Technology and Innovation Foundation, June 8, 2015), https://itif.org/publications/2015/06/09/beyond-usa-freedom-act-how-us-surveillance-still-subverts-us-competitiveness.

46. There are three key methods for website blocking: Internet Protocol (IP) address blocking, Domain Name Server (DNS) blocking, and Uniform Resource Locator (URL) blocking.

47. Claire Reilly, "AFP Using Site Blocking Laws to Target Malware," *CNET*, October 22, 2014, http://www.cnet.com/au/news/afp-using-site-blocking-laws-to-target-malware/.

48. Josh Taylor, "FOI Reveals ASIC's IP-Blocking Requests," *ZDNet*, July 1, 2013, http://www.zdnet.com/article/foi-reveals-asics-ip-blocking-requests/.

49. "Approach to Regulating Content on the Internet," Media Development Authority Singapore, August 11, 2016, http://www.mda.gov.sg/RegulationsAndLicensing/ContentStandardsAndClassification/Pages/Internet.aspx.

50. "Banned: Complete List of 857 Porn Websites Blocked in India," *Deccan Chronicle*, updated January 10, 2016, http://www.deccanchronicle.com/150803/nation-current-affairs/article/porn-ban-complete-list-857-porn-websites-blocked-india.

51. "174 Escort Services Websites to Be Blocked: State to Bombay High Court," *dna India*, April 21, 2016,

http://www.dnaindia.com/mumbai/report-174-escort-services-website-to-be-blocked-state-to-bombay-high-court-2204387.

52. For example, in 2015, France introduced a law that allows government agencies to order the blocking of websites that advocate acts of terrorism or contain images of child abuse. The legislation was brought in by revisions to the Loppsi Act, and an anti-terror bill passed by the French senate in 2014, but can now be used by the general directorate of the French police's cybercrime unit to force French Internet service providers to block sites within 24 hours, without a court order. In the United Kingdom, the government and ISPs have agreed to implement a system of blocks, similar to that used to keep child abuse material off the Internet, for websites espousing terrorism-related extremist views. Samuel Gibbs, "French Law Blocking Terrorist and Child Abuse Sites Comes Into Effect," *The Guardian*, February 9, 2015, https://www.theguardian.com/technology/2015/feb/09/french-law-blocking-terrorist-and-child-abuse-sites-comes-into-effect. the United Kingdom.

53. Nigel Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online" (Information Technology and Innovation Foundation, June12, 2018), https://itif.org/publications/2018/06/12/normalization-website-blocking-around-world-fight-against-piracy-online.

54. "Blocking and categorizing content," INTERPOL, accessed May 20, 2019, https://www.interpol.int/en/Crimes/Crimes-against-children/Blocking-and-categorizing-content.

55. Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online."

56. Ernesto, "Nearly 4,000 Pirate Sites Are Blocked by ISPs Around The World," *Torrent Freak*, February 10, 2019, https://torrentfreak.com/nearly-4000-pirate-sites-are-blocked-by-isps-around-the-world-190210/.

57. Ibid.

58. "Singapore Allows Dynamic Site Blocking in Landmark Court Ruling – Any Web Address Linking to Blocked Piracy Sites Can Now be Blocked as Well," Motion Picture Association, July 19, 2018, https://www.mpa-i.org/in_the_news/singapore-allows-dynamic-site-blocking-in-landmark-court-ruling-any-web-address-linking-to-blocked-piracy-sites-can-now-be-blocked-as-well/; Nigel Cory, "Using Dynamic Legal Injunctions and AI to Fight Piracy in Real-Time in the United Kingdom" (Information Technology and Innovation Foundation, December 3, 2018), https://itif.org/publications/2018/12/03/using-dynamic-legal-injunctions-and-ai-fight-piracy-real-time-united-kingdom

59. Cory, "The Normalization of Website Blocking Around the World in the Fight Against Piracy Online."

60. "Anti-Piracy Program FAQ," tag: Trustworthy Accountability Group, accessed July 4, 2016, https://tagtoday.net/piracyfaq/.

61. Such as Kim Dotcom (the owner of the major piracy site Megaupload.com, who was arrested in New Zealand in 2012) or the operator behind Kickass Torrents (who was arrested in Poland in June 2016), "Release for Victim Notification: United States vs. Kim Dotcom, et al," The United States Attorney's Office, Eastern District of Virginia, accessed July 18, 2016, https://www.justice.gov/usao-edva/release-victim-notification; "Owner of Most-Visited Illegal File-Sharing Website Charged with Criminal Copyright Infringement," The United States Attorney's Office, Eastern District of Virginia, July 20, 2016, https://www.justice.gov/usao-ndil/pr/owner-most-visited-illegal-file-sharing-website-charged-criminal-copyright-infringement.

62. For examples, see: "2017 Out-of-Cycle Review of Notorious Markets," Office of the United States Trade Representative, January 11, 2018), https://ustr.gov/sites/default/files/files/Press/Reports/2017%20Notorious%20Markets%20List%201.11.18.pdf

63. Nigel Cory, "How Website Blocking Is Curbing Digital Piracy Without 'Breaking the Internet'"(Information Technology and Innovation Foundation, August 2018), http://www2.itif.org/2016-website-blocking.pdf.

64. Robert Atkinson, "The Internet Is Not (Fully) Open, Nor Should It Be," *Innovation Files*, August 13, 2015, http://www.innovationfiles.org/the-internet-is-not-fully-open-nor-should-it-be/.

65. Daniel Castro and Alan McQuinn, "Unlocking Encryption: Information Security and the Rule of Law"(Information Technology and Innovation Foundation, March 14, 2016), https://itif.org/publications/2016/03/14/unlocking-encryption-information-security-and-rule-law

66. Encryption is the act of scrambling the data, and decryption is the act of restoring the data to its original form. To encrypt or decrypt, a key is needed. Cryptography can be described as a discipline which embodies principles, means, and methods for the transformation of data in order to hide its information content, prevent its undetected modification and prevent its unauthorized use. A cipher (or cypher) is an algorithm that transforms meaningful data into seemingly random data, and back again, when needed. For further information on cybersecurity and trade, see: Sweden's National Board of Trade, *The Cyber Effect: The Implications of IT Security Regulation on International Trade* (Stockholm, June 2018), https://www.kommers.se/Documents/dokumentarkiv/publikationer/2018/The-Cyber-Effect.pdf.

67. Trevor Tim, "The FBI Used to Recommend Encryption. Now They Want to Ban It," *The Guardian*, March 28, 2015, https://www.theguardian.com/commentisfree/2015/mar/28/the-fbi-used-to-recommend-encryption-now-they-want-to-ban-it; Liz Gannes, "Obama: 'There's No Scenario in Which We Don't Want Really Strong Encryption'," Recode, accessed January 4, 2016, http://recode.net/2015/02/13/obama-theres-no-scenarioin-which-we-dont-want-really-strong-encryption/.

68. Castro and McQuinn, "Unlocking Encryption: Information Security and the Rule of Law."

69. U.S. Department of Energy, "Secure Data Transfer Guidance for Industrial Control and SCADA Systems," PNNL20776, September 2011, at http://www.pnnl.gov/main/publications/external/technical_reports/PNNL-20776.pdf.

70. Chris Jaikaran, "Encryption: Frequently Asked Questions," Congressional Research Service, September 28, 2016, https://fas.org/sgp/crs/misc/R44642.pdf.

71. "Summary of the HIPAA Security Rule," *HHS.gov*, https://www.hhs.gov/hipaa/for-professionals/security/laws-regulations/index.html.

72. Lisa Lambert and Jeff Mason, "Obama Backs Away From Law to Access Encrypted Information," *Reuters*, October 10, 2015, https://www.reuters.com/article/us-usa-cybersecurity-legislation/obama-backs-away-from-law-to-access-encrypted-information-idUSKCN0S40VN20151010.

73. Kim Zetter, "Encryption Is Worldwide: Yet Another Reason Why a US Ban Makes No Sense," *Wired*, February 11, 2018, https://www.wired.com/2016/02/encryption-is-worldwide-yet-another-reason-why-a-us-ban-makes-no-sense/ and "Dutch Government Says No to 'Encryption Backdoors'," *BBC News*, January 7, 2016, https://www.bbc.com/news/technology-35251429

74. These attempts include banning the export of certain types of encryption, undermining encryption standards, building

backdoor software and hardware, asking the private sector to develop key escrow or intercept capabilities, and developing capabilities to use brute force to decrypt encrypted data. See Jay Stowsky, "Secrets or Shields to Share? New Dilemmas for Dual Use Technology Development and the Quest for Military and Commercial Advantage in the Digital Age," Berkeley Roundtable on the International Economy, February 21, 2003, http://escholarship.org/uc/item/89r4j908; Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard," *Scientific American*, September 18, 2013, http://www.scientificamerican.com/article/nsa-nist-encryption-scandal/; Evan Perez and Shimon Prokupecz, "First on CNN: Newly Discovered Hack Has U.S. Fearing Foreign Infiltration," *CNN*, December 19, 2015, http://www.cnn.com/2015/12/18/politics/juniper-networks-usgovernment-security-hack/; "Discovering IT Problems, Developing Solutions, Sharing Expertise," U.S. National Security Agency, October 30, 2015, https://www.nsa.gov/public_info/news_information/2015/ncsam/discovering_solving_sharing_it_solutio ns.shtml; Steven Levy, "Battle of the Clipper Chip," *The New York Times*, June 12, 1994, http://www.nytimes.com/1994/06/12/magazine/battle-of-the-clipper-chip.html.

75] Larry Greenemeier, "NSA Efforts to Evade Encryption Technology Damaged U.S. Cryptography Standard;" Joseph Menn, "NSA Says How Often, Not When, It Discloses Software Flaws," *Reuters*, March 30, 2015, http://www.reuters.com/article/us-cybersecurity-nsa-flaws-insightidUSKCN0SV2XQ20151107#QZF5OuhmEg2KCeA5.97.

76] Aaron Tan, "Apple Challenges Australia's Proposed Decryption Law," *Computer Weekly*, October 15, 2016, https://www.computerweekly.com/news/252450584/Apple-challenges-Australias-proposed-decryption-law.

77] Castro and McQuinn, "Unlocking Encryption: Information Security and the Rule of Law."

ABOUT THE AUTHORS

Nigel Cory is associate director, trade policy, with the Information Technology and Innovation Foundation. He previously worked as a researcher at the Sumitro Chair for Southeast Asia Studies at the Center for Strategic and International Studies. Prior to that, he worked for eight years in Australia's Department of Foreign Affairs and Trade, which included positions working on G20 global economic and trade issues and the Doha Development Round. Cory also had diplomatic postings to Malaysia, where he worked on bilateral and regional trade, economic, and security issues; and Afghanistan, where he was the deputy director of a joint U.S./Australia provincial reconstruction team. Cory holds a master's in public policy from Georgetown University and a bachelor's in international business and a bachelor's in commerce from Griffith University in Brisbane, Australia.

Robert D. Atkinson is the founder and president of the Information Technology and Innovation Foundation. He is also the coauthor of the book *Innovation Economics: The Race for Global Advantage* (Yale, 2012). Atkinson received his Ph.D. in city and regional planning from the University of North Carolina at Chapel Hill in 1989.

Daniel Castro is vice president of ITIF and director of ITIF's Center for Data Innovation. His research interests include health IT, data privacy, e-commerce, e-government, electronic voting, information security, and accessibility. Before joining ITIF, Castro worked as an IT analyst at the Government Accountability Office, where he audited IT security and management controls at various government agencies. He has a B.S. in foreign service from Georgetown University and an M.S. in information security technology and management from Carnegie Mellon University.

ABOUT ITIF

The Information Technology and Innovation Foundation (ITIF) is a nonprofit, nonpartisan research and educational institute focusing on the intersection of technological innovation and public policy. Recognized as the world's leading science and technology think tank, ITIF's mission is to formulate and promote policy solutions that accelerate innovation and boost productivity to spur growth, opportunity, and progress.

For more information, visit us at www.itif.org.