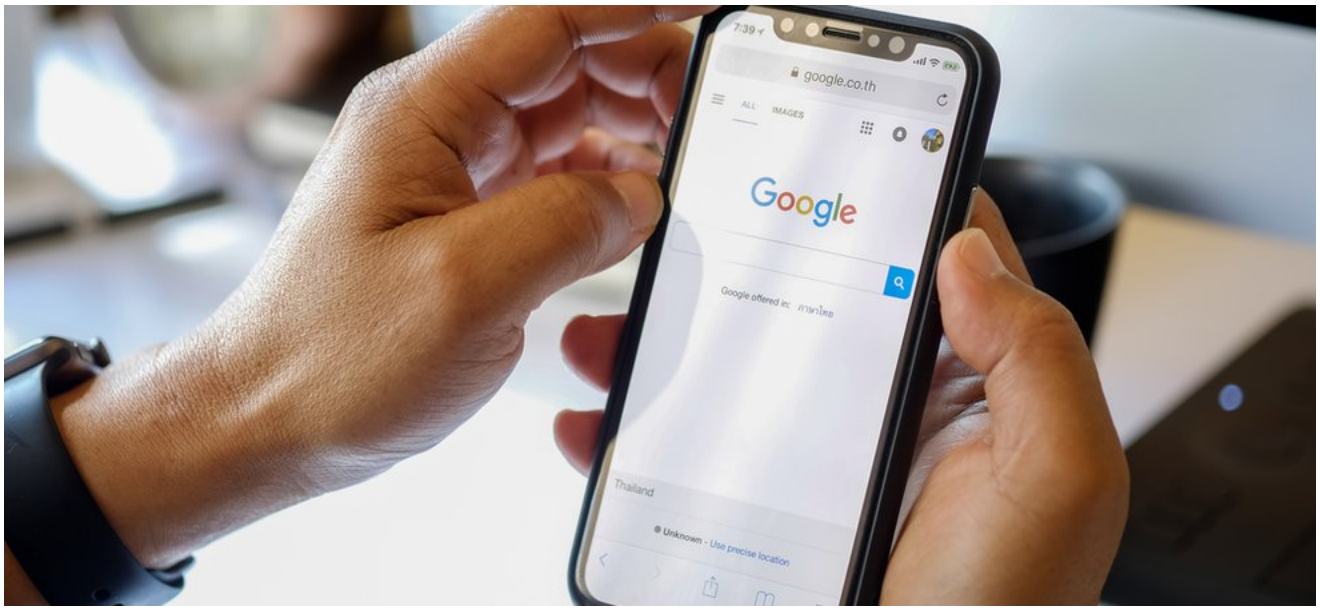
NEW AMERICA

THE HOWARD BAKER FORUM



December 2019

Global Data Governance

Concepts, Obstacles, and Prospects

Samm Sacks & Justin Sherman

Last edited on December 09, 2019 at 2:22 p.m. EST

Acknowledgments

The authors would like to thank Jennifer Daskal, Professor of Law at American University and Scholar-in-Residence at New America, and Bill Deckelman, EVP and General Counsel of DXC Technology, for co-chairing the roundtable discussion that informed the basis of this report and for providing legal and technological insights. The authors would also like to thank all the experts, whose identity shall remain anonymous, who participated in the roundtable discussion. We would like to extend an additional thanks to Sadanori Ito, Special Advisor of Japan's Ministry of Economy, Trade & Industry (METI) and Director of Japan External Trade Organization (JETRO) NY, for his governmental and diplomatic perspectives, and to Jennifer Daskal, Nigel Cory, and David Hoffman for their feedback on an earlier draft of this document.

About the Author(s)

Samm Sacks is a Cybersecurity Policy and China Digital Economy Fellow at New America. Her research focuses on emerging information and communication technology (ICT) policies globally, particularly in China.

Justin Sherman is a Cybersecurity Policy Fellow at New America.

About New America

We are dedicated to renewing America by continuing the quest to realize our nation's highest ideals, honestly confronting the challenges caused by rapid technological and social change, and seizing the opportunities those changes create.

About Cybersecurity Initiative

The goal of New America's Cybersecurity Initiative is to bring the key attributes of New America's ethos to the cybersecurity policy conversation. In doing so, the Initiative provides a look at issues from fresh perspectives, an emphasis on cross-disciplinary collaboration, a commitment to quality research and events, and dedication to diversity in all its guises. The Initiative seeks to address issues others can't or don't and create impact at scale.

About the Howard Baker Forum

The Howard Baker Forum was founded by former Senator Howard Baker in Washington, D.C. to provide a platform for examining specific, immediate, critical issues affecting the nation's progress at home and its relations abroad.

Contents

Introduction

Policymakers around the world are grappling with daunting challenges for securing data (digital information) and addressing a host of issues raised by cross-border data flows. Addressing these issues at the global level is made harder by the fact that there is tremendous debate and uncertainty over the way in which governments should interact with the private sector, other governments, and international institutions and forums in discussing how to piece together their data policies, standards, and laws in order to form a framework for data governance.

The rules for how governments and companies collect data, use it to generate insights (i.e., value), and then store and protect it matter across all sectors of the economy. Manufacturing, finance, healthcare, and other industries are increasingly becoming "data-centric" in that they rely on vast quantities of digital information to conduct business. Data sent across global internet and telecommunications networks enables products and services from email and customer management software to cutting-edge technologies like artificial intelligence, the Internet of Things (IoT), and 3D printing. Data presents many opportunities, from increased economic growth to improved medicine to better public safety, but it also presents many risks around data misuse and abuse, such as with data privacy violations, algorithmic unfairness, and mass surveillance.

Data presents many opportunities, from increased economic growth to improved medicine to better public safety, but it also presents many risks around data misuse and abuse, such as with data privacy violations, algorithmic unfairness, and mass surveillance.

To begin to address this set of questions around data governance, Japanese Prime Minister Shinzo Abe launched the "Osaka Track" at the G20 summit in June. The objective of the initiative is to create a framework to promote cross-border data flows with enhanced protections and safeguards. Twenty-four countries, including China and the United States, signed a statement affirming the concept of free data flows. India was among those countries who did not.

The most challenging part of the Osaka initiative lies ahead. For the initiative to have any meaning at all—as the global data landscape becomes more fraught and fragmented over time—there needs to be substantive discussion of the hard issues.[1]

The Howard Baker Forum and New America convened an expert roundtable in Washington, D.C. on October 3 with the aim of charting a path forward in global data governance. This report aims to capture the main takeaways from that discussion by setting out the debates that underpin the key issues. While the outcome of these debates is not yet clear, the goal of the report is to identify the factors that would need to be addressed in a global data governance framework. It is a starting point meant to guide future discussions. Because the discussion operated under Chatham House Rule, we are the only participants identified in this paper, though the attendees were a diverse group of experts spanning government, private industry, think tanks, and academia. We draw on their expertise at the roundtable discussion in this report.

The first section of this report lays a conceptual foundation by defining what we mean by the terms "data" and "data governance." Often, misunderstandings about terminology can lead to experts talking past one another and to the creation of obstacles from the start. The second section then defines what we call the different "levers" that make up data governance regimes (e.g., trade agreements, laws, standards, technical tools, etc.) at the super-national, national, and sub-national levels.

The following three sections each focus on key issues that emerged from the discussion:

1. Should a global data governance regime start from the basis that free data flows are (a) inherently beneficial and (b) inevitable?

2. What is the proper relationship between the different levers of data governance?

3. In designing a coalition of countries for whom a set of data flow rules apply, how big should the coalition be, and which countries should belong to it?

Finally, we conclude with a discussion of what research questions need to be addressed in order to move forward in creating an international framework in line with Prime Minister Abe's vision.

Defining Data Governance

The term "data" refers to information created, processed, saved, and stored digitally by a computer in ones and zeros—or binary format. Network connections or devices allow this data to be transferred from one computer to another. There is also a distinction that needs to be drawn between "data" (machine-readable ones and zeros, or "code") and "information" (what that data means to humans).[2] Such data and information can have different implications depending on their type (e.g., pertaining to finance, health, social media, law enforcement, etc.).

Based on these definitions and distinctions, we generally define data governance as the rules for how governments interact with the private sector—as well as with other governments—when it comes to managing data to determine who has access to it and the ways in which those with access can use it. As previously articulated, this includes the design and enforcement of standards, policies, and laws.

We understand that the term "data governance" has many different meanings depending on the context and the perspective of various stakeholders. For the purposes of our roundtable, our goal was to have a structured discussion about data governance as it applies to the following three issues (in no particular order):

1. **National security/law enforcement:** a government's interest in ensuring access to data for purposes of domestic and international security; other governments' converse concerns about misuse of that data; and desires to protect data against foreign collection;

2. **Economic growth/innovation:** objectives to create and access large databases of data for research and development of data-intensive technologies like machine learning/artificial intelligence, as well as for cross-border transactions and ecommerce; and

3. **Content moderation policies and practices:** competing demands on what is and is not permissible content, and possible ways to manage that conflict while also ensuring the free flow of data.

Across these three distinct areas, there are different types of tools or "levers" that set the terms around how data is collected, used, transferred, and stored. These levers essentially set the bar for concepts such as "trust" in Prime Minister Abe's concept of "Data Free Flow with Trust." Since the concept of trust is quite vague (with significant debate regarding the degree to which regulation even enhances trust),[3] a core objective of this project is to consider how the various levers at play

can and should be configured to achieve certain safeguards. We discuss these levers in the next section.

Additionally, the issue of how governments support data flows across borders—or conversely, how governments restrict those flows—is a major focal point across each of the three aforementioned areas of data governance. The term "data localization," for example, appears frequently in policy discussions to mean restrictions on the ability of firms to transfer data from domestic sources to foreign countries—in other words, the opposite of free data flow.[4] In reality, the term could have several different meanings. There is a spectrum when it comes to severity.

On the most permissive side of the spectrum is "mirroring," where a country requires that a copy of data be stored on a server within that country before it's allowed to be sent out. Partial data localization could mean that restrictions only exist on certain domain names or on data from specific sectors like health or finance. China's system is stricter than that of many other countries in that the government requires firms to store certain kinds of data on servers inside the country, while allowing transfer in or out under certain conditions. There still appears to be a regulatory gray zone in which multinationals in China can send certain kinds of data outside the country, but it is not clear the extent to which this will be the case in the future, given the significant weight given to national security in Beijing's approach to data regulation.

In other cases, however, data localization may be implemented in an even stricter manner by requiring local storage and local processing while prohibiting outbound transfer altogether. This could mean foreign firms cannot access and use data to create value outside of that geographic area. Russia and India already take such an approach with some kinds of data (i.e., payment data in India's case), and other countries are increasingly considering it. But at least for now, with a few exceptions, most governments have yet to notably implement these stricter forms of data localization.

The above pathways all fall under the "data localization" umbrella of policy options. But localized storage and processing requirements are by no means the only policy option available for limiting free flows on data; countries could also potentially implement some form of algorithmic filtering in order to allow or disallow certain kinds of data, possibly even from certain places, to flow into or out of their borders.[5] This could focus on anything from sensitive personal health information to political online content, depending on factors such as the government's policy priorities and its technical capabilities.

We discuss the key challenges for enabling cross-border data flows as part of Theme 1 later in this report. Before that, however, we turn in the next section to the "levers" of data governance and their relationships at super-national, national, and sub-national levels.

The Levers of Data Governance

Levers of data governance exist at super-national, national, and sub-national levels. These include bilateral, regional, and multilateral trade agreements, and a broad range of data-related laws, regulations, standards, and norms. Litigation, particularly class action lawsuits, also has a role to play. All these levers are ways in which governments, corporations, and other key actors in global data governance can technically influence how data flows and is stored, and ways in which they can similarly exert influence in legal and regulatory fashions.

First and foremost is the technical element: governments cannot make decisions about data governance in isolation from the technical layers of the internet. Despite wishes to restrict access to encrypted messaging apps, for instance, the Russian government has proven unable to effectively block the messaging app Telegram from within Russian borders due to technical challenges.[6] Countries looking to design data governance regimes that exclude others from accessing certain data located on websites hosted within their borders, to use another example, cannot do so without consideration for how the internet is currently designed to globally route information. Standards, or technical rules around issues like web traffic security and internet protocol interoperability, play a critical role here. This all means that in practice, limits on free data flows are not simply a matter of government power or legal authority, but also reflect government and corporate technical capabilities—its own subset of the levers of data governance.

In order for governments and firms to influence technical elements of the internet, such as data flows across internet architecture, they leverage policies, laws, and regulations. Even if these rules do not specify exactly how certain practices should be executed in code, they may at least specify certain technologies that should be used for certain purposes, or which organizations are in charge of executing the technical steps. For example, at one time, Brazil required the use of a local email service instead of Outlook, but the effort failed because it wasn't supportive of attachments and other functions. The policy requirements were ineffective because the technology was simply an obstacle to human and organizational performance.

Technical protocols and standards remain an integral yet poorly understood part of this conversation about the "levers" of data governance. Deeper study and mapping of the standards landscape across categories such as internet architecture, company activities, people, and governments would be helpful as a basis for any international framework.[7]

At both technical and regulatory levels, there is a need to maintain some level of interoperability between different countries' internet systems and governance regimes—lest, for example, global internet speeds greatly decline or certain data

flows to certain destinations halt altogether. Again, such a discussion should account for how the internet currently works; even if data governance is discussed differently from internet governance, or as a somewhat overlapping but somewhat separate issue, the governance of data flows is inextricably linked to how the global internet operates.

It remains an open question how these issues of interoperability should be handled between countries. For instance, the handling of cross-border data flow and cybersecurity issues at the World Trade Organization (WTO) has been fraught with complications. This includes uncertainty about whether current WTO rules (written in the pre-internet era) apply or not to digital trade issues. Related to that, there have also been disputes over whether certain regulations (i.e., data localization policies) violate member countries' WTO obligations.[8] Rulemaking in bodies like the WTO is going to come with its own set of challenges.

The costs of fundamental incompatibility between systems are not trivial. Conflict could hinder the free flow of data (see Theme 1, the next section), limit the aggregation and use of data to drive innovation, and impose heavy costs on corporations that must duplicatively store the same kinds of data in many different geographies.

Participants identified a number of challenges in creating a global framework using different levers of data governance, including:

- **Lack of quantifiable indicators:** Unlike with physical goods, there are no clear and universal ways to quantify and track the volume of data flows against the value of those flows.

- **Classification challenges:** A question that emerged from discussion is whether regulation should treat different kinds of data separately (rather than treating all data the same in bulk). In other words, not all data flows should be treated the same. Sensitive personal information (e.g., from healthcare), manufacturing data (e.g., from factories), law enforcement data, and national security data (e.g., from the Five Eyes intelligence alliance) are in many cases different, even if related or overlapping, and should be handled as such. The question then becomes who has the right to classify that data, and whether this should be a kind of "self-declaration" by companies or come from a regulatory body (which likely would lead to industry pushback). The role of industry and governments in determining what kind of data would be classified as personal data, for example, remains an open question. Related, there is also a separate ongoing discussion as part of the Budapest Convention on Cybercrime about how to handle subscriber data, but not the actual content of communications.

- **Conceptual differences:** There is a need for a comparative regional analysis on the state of play to understand what levers exist to date, and the conceptual or philosophical foundation upon which those levers are based. A key question is whether an international framework can be created despite these differences.

Different regions may use distinct levers for governing concepts like "privacy" and "security." For example, the term "data protection" in the European context may be interchangeable with notions of individuals' autonomy over their own data—something more commonly associated with the term "privacy"—while in the Chinese context, data protection tends to refer more to restrictions put in place to secure data against criminal actors, while allowing unchecked government access to personal data. China may not be unique in this aspect as countries including India, Singapore, and Vietnam similarly have data protection laws or are considering data protection bills that apply to the private sector but not the government.

There is a need for further study into the relationship between privacy and cybersecurity when it comes to data regimes. Will these two concepts increasingly blur, or should they be kept distinct? In the United States, cybersecurity law has tended to grow out of privacy law. The exception is California's IoT security law, which centers on the protection of the device rather than personal data.

Ultimately, the levers of data governance are also part of broader differences in how countries conceptualize and operationalize national and cyber security, and what impact this has on the use of data in the digital economy. There are also differences in how governments balance objectives around the rights of individuals to control their data and the desire of private-sector players to profit and innovate.

Existing data governance regimes around the world all strike a somewhat different balance in the triad of state, individual, and corporate interests. Is it possible to create a meaningful super-national framework among various governments if we take as a given that national levels are likely to start from different places in this triad?

The issue becomes more complex when we consider that some governments may have more sub-national debate than others when it comes to this triad. For example, while there is often more internal debate within China's bureaucracy on data issues than gets acknowledged from the outside, the reality is that it will be easier for a country like China to have a more cohesive organizing principle (i.e., state security) that overrides all others interests at play in the triad. The question, then, is whether other systems are able to effectively balance tensions by coming up with their own cohesive view of data governance (i.e., considering economic strength as distinct from state security).

Theme 1: Growing Restrictions on Free Data Flows

At the most basic level, policymakers seeking to create a global data governance framework must address a number of fundamental questions when it comes to transferring data across borders: To what extent does data flow freely across borders today? Should the free flow of data exist in the future? Are free data flows beneficial and inevitable? If so, what safeguards need to be in place and what obstacles need to be overcome to create interoperability across regions with different perspectives on the issue?

Countries that restrict cross-border data transfers could have several (often overlapping) motivations for doing so. The first reason could be to increase some notion of security (based on the assumption that data's location is more important for its security than the measures taken to secure it). Data restrictions could also be motivated by a government's desire to impose content-based controls on communications that occur online. Another possible driver is to promote domestic digital industries by ensuring that value from local citizen data remains in-country. Governments may also seek to enhance their ability to access data for law enforcement purposes as well as for other political or social uses by security and intelligence services.[9]

Most experts agreed that the free flow of data is more or less the status quo today (though it may not be that way forever). While there are filtering mechanisms in place on internet data in various parts of the world, and there are also data localization policies that mandate data stays in certain geographies, the majority of data does flow relatively uninhibited over the global internet because (a) existing restrictions do not block all kinds of data or are enforced unevenly, and (b) there are many technical barriers to enforcement, as demonstrated by the use of internet censorship work-arounds (i.e., Virtual Private Networks) in countries like China and Russia. That said, there are a range of geolocation-based internet traffic blocking protocols, data transfer restrictions, and other measures being imposed all around the world that are restricting data flows across borders.

To maintain free flows of data in the future, the question is what rights and obligations should come with the movement of data. In other words, what levers of data governance should be used to establish "trust" at the center of Prime Minister Abe's vision?

Answering this question requires first taking into account fault lines or areas in which there may be conflict. According to Sadanori Ito, the official from Japan's Ministry of Economy, Trade and Industry who was in charge of the digital component of the G20 Leaders' Statement, the three main fault lines are as follows:

1. Advanced economies vs. emerging market economies

2. United States (and European Union) vs. China

3. United States vs. European Union

First, when it comes to conflict between advanced and emerging economies, some governments are pushing for restrictions on data flows based on the premise that countries like the United States reap a disproportionate share of benefits. While policymakers and industry groups in Australia, Canada, Japan, Singapore, parts of Europe, and elsewhere tend to advocate free data flows to promote global commerce, other stakeholders in emerging economies like India argue that this is not necessarily in their best interest. India's unwillingness to sign onto the G20 Osaka Agreement underscores a trend of pushing back against "data colonialism" by western tech giants, arguing that restrictions on cross-border data transfer may bolster the competitiveness of India's domestic startup ecosystem, protect the privacy of Indian citizens, and position India as a global player in data regulation.[10]

But not all emerging economies subscribe to India's view of "data nationalism," instead embracing rules that support data flows, such as among "Pacific Alliance" members in Latin America (Chile, Colombia, Mexico, and Peru), Vietnam, and Malaysia.[11] However, if India's approach advances domestically, and other countries take a similar path, restrictions on data flows could become more of a norm for the global internet (or at least large parts of it).

The second fault line is competition between the United States and China, particularly when it comes to data-intensive technologies like artificial intelligence, and underpinning architecture like 5G telecommunications networks that will enable the deployment of these technologies. Washington and Beijing are increasingly concerned about access to data on their respective citizens by the other government. Many different forms of restrictions on data flows could thus be implemented as a result.

Both the United States and China are also rolling out new regulatory tools to limit data flows based on national security concerns. China's Cybersecurity Law introduced provisions that would require certain kinds of data ("important data" and "personal data" produced by critical information infrastructure operators) to be stored inside China or undergo a security audit before being sent out.[12] Meanwhile, the U.S. government has made access to "sensitive data" on U.S. citizens a major new focus of reviews of transactions under the Committee on Foreign Investment in the United States. Sen. Josh Hawley (R-Mo.) is working on legislation that would prohibit data transfer to a list of blacklisted countries like China.[13]

The third major fault line is between the United States and Europe. The Court of Justice of the European Union already once—and may very well again—restricted data flows from Europe to the United States because of a concern about the

absence of sufficient privacy protections in the United States. The European Union also takes a different approach to the United States in dealing with data flows and privacy issues in trade agreements: excluding privacy from trade agreements, instead dealing with them in a separate legal arrangement under the General Data Protection Regulation (GDPR) called an "adequacy agreement" to allow for data exchange with the European Union.

One point of convergence, however, between U.S. and European officials appears to be shared concerns over Beijing's data regime. EU officials have indicated that China may never be eligible for "adequacy." Chinese companies may find that it's impossible to comply with GDPR and China's cybersecurity law at once. Although those who drafted China's data-privacy rules looked to GDPR as a model, the version of GDPR they created for China's political system—where the government has expansive surveillance authorities—makes it hard to imagine how the Chinese and European systems could ever be reconciled.[14] Therefore, as EU officials grow increasingly concerned about China's approach, there could be more alignment between Europe and the United States.

As conflict over data grows more fraught, data may not flow freely across all of these fault lines in the future. In other words, free flow of data may only be possible among certain groups, or "coalitions" (as discussed in Theme 3).

The question of legal nexus underpins the conflict over what safeguards should be in place to facilitate cross-border data flows—that is, determining responsibility and accountability when multiple countries assert jurisdiction over the same data: the nationality of the individuals and organizations owning data, service providers storing data, individuals and organizations accessing data, and individuals described in the data.[15] Some argue that as long as a firm operates in a given country, then that country's data rules apply and should be enforced. Doing so would then negate the need for data localization by that country to maintain control over its own data. In the case of a crime, for example, the most important factor would be where the investigating entity is located rather than where the data is located. This leads into the next section, where we discuss the relationship between domestic and international levers.

Theme 2: Relationship Between Domestic and International Levers

When overarching common principles in international data frameworks contradict national laws, there is often little benefit in having convergence.[16] A central challenge is grappling with the proper relationship between the international and domestic levers of data regimes.

Several experts suggested that there is already a lack of compatibility between domestic and international levers around data governance. One participant noted that many countries' international engagement on these data issues (free flows, law enforcement access to data, content moderation, etc.) is hampered by a lack of domestic consensus on the policy outcomes that the country should try to achieve. Even a relatively comprehensive data governance regime like GDPR arguably fits into this category, insofar as various motivations like consumer data protection, pushback against American tech firms, and mandating better tech company cybersecurity may have been in conflict, to some degree, in the final law.

Another participant argued that there will always be a patchwork of laws around any issue. In the early days of internet governance—and, more or less, still today—most countries treated the governance of the (then, relatively) global network as a domestic issue and passed laws as such; there is a growing recognition of the need for multilateral efforts in this regard.

With data governance, therefore, countries must consider the ways in which domestic and/or international levers could work together to most appropriately and effectively manage worldwide data flows. Otherwise, states may risk harmfully imposing wide-ranging laws on global telecommunications systems that end up negating the benefits of convergence. As Daphne Keller, Intermediary Liability Director at the Stanford Center for Internet & Society (disclaimer: she did not participate in this roundtable), noted recently, it seems "perfectly reasonable" for companies to comply with certain data rules in different jurisdictions, "but that's exactly the problem: every court in every country will want to do the same thing."[17]

With data governance, therefore, countries must consider the ways in which domestic and/or international levers could work together to most appropriately and effectively manage worldwide data flows.

Participants identified a number of challenges moving forward:

- **Designing the patchwork:** Should certain countries work together with certain other countries to make their regulatory patchworks compatible? Should countries make their regulatory regimes compatible with as many others as possible? Should sovereignty and individual priorities instead be the primary concern for governments? This relates to the question of a coalition of countries that work together to enforce certain free data flow rules, which we discuss in the next section.

- **Identifying the international bodies:** Which international bodies might be appropriate venues through which to address certain data governance issues? For instance, how might security exceptions in the WTO constrain the ability of states to effectively use the WTO to enforce free-data-flow policies?

- **Maintaining a relatively global data system:** If some countries should desire to maintain relatively free data flows, how do they manage relationships between domestic and international levers so as to not impose too many restrictions on global networks? How much regulation is too much regulation?[18]

This leads to our discussion in the next section of a third theme: the building of coalitions.

Theme 3: Framework Coalitions

Which countries should be included in an international data framework? How many members should be included? What are the consequences of constraining group membership? Should different coalitions be formed for different subsets of data governance? The discussion did not come to a definitive answer on these questions, so much as underscore the critical sets of trade-offs involved in drawing these lines. Understanding these trade-offs will be an important next step in determining the composition of data governance framework coalitions.

Specifically, there are arguments that support keeping the coalition small in order to have legally-binding, enforceable rules that protect the role of data flows in digital trade and innovation, while providing narrow exceptions for privacy, cybersecurity, national security, and other data-related issues. The idea is that countries may be more willing to create binding international agreements with other members who they already generally "trust" and who they know share a broadly similar approach to data governance (thus reducing the likelihood they'll use exceptions as a disguise for protectionism).[19]

But the risk of doing so is that those countries excluded from membership in a framework coalition could align in a competing bloc or competing blocs.

In determining the composition of the coalitions, the first question is how to account for different interpretations of the concept of "free" data flows. Even relatively free and democratic societies, one expert pointed out, draw lines somewhere on free information flows, such as laws that restrict the online transfer of intellectual property. This expert also pointed out the global rise in cyber sovereignty pushes over the last several years—spanning regulatory changes (like state control of internet service providers [ISPs] and data localization laws) as well as technical changes (like IP blacklisting and DNS filtering)—as evidence that there is not at all agreement on free data flows. Countries might consider restrictions on the transfer of intellectual property-related data to be an acceptable limit on free data flows, but may not feel the same about deep packet inspection (DPI) filtering focused on content on a country's major internet gateways (which is currently implemented in China's Great Firewall). If agreement on DPI filtering on internet gateways is *not* a prerequisite for coalition membership, then the size of the coalition could grow and accommodate China and the United States at once, for example.

This leads to the second question: should the parameters of coalition membership reflect a country's broader preferences around internet and data governance, given that those preferences themselves are often reflective of a country's overall governance structures and political goals?[20] If the answer is yes, then either the coalition needs to be small or forming a data-sharing coalition may not be achievable at all.

One participant raised the question of what happens, as some countries have discussed, if the European Union and countries like the United States, Japan, and India form a data governance framework—that is, design an exclusively compatible data governance regime—which excludes China and many others. Will these other countries then be left without market access to data important to emerging technologies like 5G telecommunications, the IoT, and machine learning/artificial intelligence? Will they be inclined to then move towards a Chinese-style data governance model that might be more globally restrictive in terms of data flows, because they have nowhere else to turn? This could accelerate a move already underway by some countries attracted to China's approach to digital development (i.e., enhanced controls over the internet with a thriving digital economy). The question of how the creation or formation of coalitions may inherently create out-groups was by no means answered during the roundtable.

Participants identified a number of challenges moving forward:

- **Designing or forming coalitions:** Does the creation of a global data governance framework have to begin with the formation of membership groups? If so, which countries should design which kind of coalition with which other countries? How could they work to ensure compatibility in their data governance regimes within the coalition? Or will these coalitions form naturally, and are there already mechanisms by which these coalitions can then develop data governance regimes to protect certain objectives?

- **Creating out-groups:** What are the trade-offs that could arise if some countries are excluded from coalitions? Will this incentivize them to design compatible/compliant data governance regimes—for instance, those with certain privacy protections—or is it only going to isolate them? Will this grouping into coalitions encourage the fracturing of global data flows, and, in fact, undermine the very point of forming coalitions to protect data flows in the first place?

Conclusion

We hope this report lays a foundation for delving deeper into what issues need to be assessed in order to create a global data governance framework. It is meant as a starting point that provides analysis of the current landscape and debates surrounding data governance. As a next step, we recommend a comprehensive study focused on the following research questions:

- Starting points—what are the current geopolitical views, technical realities, historical foundations, and cultural perspectives with which different countries are approaching questions of data governance?

- Privacy and cybersecurity—how are these concepts defined and how do they relate to one another in existing data governance regimes in different countries, and will they become increasingly inseparable in data regulations in the future?

- Interoperability—is it possible, technically and legally, for different countries' data governance regimes to be somewhat compatible to maintain some data flow interoperability, and if so, should this interoperability be coordinated through bilateral arrangements, multilateral arrangements, or international bodies?

- Coalitions—should certain countries be deliberately included or excluded in coalitions of countries who agree to design interoperable data governance regimes to ensure relatively free data flows, and if so, what are the implications of these decisions?

- Processes and institutions—where and how should global data governance regimes be developed and implemented in coordination (or perhaps in conflict) with one another, from multilateral talks and treaties to bodies like the WTO?

In examining all of these issues, a possible conclusion might be that data (specifically certain types of data) should only flow freely among or within certain coalitions of countries. And if we assume that not all data should be treated as equal, then different coalitions may be formed for different types of data.

The governance of data flows has always been captured, to varying extents, in conversations about internet governance writ large, but governing data flows will become greatly more important over the next several years as technologies like the IoT, 5G telecommunications, and machine learning/artificial intelligence continue to be researched, developed, and more widely and deeply deployed in

various facets of life all around the world. These technologies generate/collect large volumes of data and/or are underpinned by data, such as with wearable IoT devices tracking biometric information or facial recognition systems needing large datasets to function precisely and accurately. Among the many questions raised by this technological explosion will be governing data in ways that balance concerns and issues at play, including consumer privacy, technological innovation, economic growth, content moderation, and law enforcement access to data.

Notes

1 This is based on a framing paper developed for the roundtable discussion, which itself was based on our article: Samm Sacks and Justin Sherman, "The Global Data War Heats Up," *The Atlantic*, June 26, 2019, https://www.theatlantic.com/international/archive/2019/06/g20-data/592606/

2 This is a distinction one of us previously established in: Robert Morgus and Justin Sherman, "The Idealized Internet vs. Internet Realities," (Washington DC, New America, 2018) https://www.newamerica.org/cybersecurity-initiative/reports/idealized-internet-vs-internet-realities/ 27

3 Daniel Castro and Eline Chivot, "The GDPR Was Supposed to Boost Consumer Trust. Has it Succeeded?" *European Views*, June 6, 2019, https://www.european-views.com/2019/06/the-gdpr-was-supposed-to-boost-consumer-trust-has-it-succeeded/

4 World Trade Report "How do we prepare for the technology-induced reshaping of trade?" (2018) https://www.wto.org/english/res_e/publications_e/wtr18_4_e.pdf

5 We have both noted, in a range of places and contexts, how hypothetical limitations on the flow of AI-related data around the world (i.e., code for neural networks, training data sets, etc.) stand in stark contrast to the current state of AI research, which remains incredibly open. See: Justin Sherman, "U.S. Tech Needs Hard Lines on China," *Foreign Policy*, May 3, 2019, https://foreignpolicy.com/2019/05/03/u-s-tech-needs-hard-lines-on-china-artificial-intelligence-technology-microsoft-google-defense/ Samm Sacks, "Smart Competition: Adapting U.S. Strategy Toward China at 40 Years," Testimony before the House Foreign Affairs Committee, May 8, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/samm-sacks-testifies-house-foreign-affairs-committee-smart-competition-china/ and Justin Sherman, "The Pitfalls of Trying to Curb Artificial Intelligence Exports," *World Politics Review*, June 6, 2019, https://www.worldpoliticsreview.com/articles/27919/the-pitfalls-of-trying-to-curb-artificial-intelligence-exports

6 Vlad Savov, "Russia's Telegram ban is a big, convoluted mess," *The Verge*, April 17, 2018, https://www.theverge.com/2018/4/17/17246150/telegram-russia-ban

7 Relevant standards organizations include the International Organization for Standardization (ISO), International Electrotechnical Commission (IEC), Internet Engineering Task Force (IETF), and the U.S. National Institute of Standards and Technology (NIST).

8 For a snapshot of this issue set and some related disputes in recent years, see: Chris Mirasola, "U.S. Criticism of China's Cybersecurity Law and the Nexus of Data Privacy and Trade Law," *Lawfare*, October 10, 2017, https://www.lawfareblog.com/us-criticism-chinas-cybersecurity-law-and-nexus-data-privacy-and-trade-law and Joshua P. Meltzer and Cameron F. Kerry, "Cybersecurity and digital trade: Getting it right," Brookings Institution, September 18, 2019, https://www.brookings.edu/research/cybersecurity-and-digital-trade-getting-it-right/ Also see: https://www.kommers.se/Documents/dokumentarkiv/publikationer/2016/Protectionism%20in%20the%2021st%20Century_webb.pdf

9 The authors thank Nigel Cory for his analysis on motivations driving data localization as presented at Stanford University on October 30, 2019. For more details, see: Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust,'" Information Technology & Innovation Foundation, May 27, 2019, https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust

10 Justin Sherman, "India's Data Protection Bill in Geopolitical Context," New America, July 10, 2019, https://www.newamerica.org/cybersecurity-

initiative/c2b/c2b-log/indias-data-protection-bill-geopolitical-context/

11 Brazil also agreed to similar provisions in its FTA with Chile from late last year. Costa Rica and Nigeria (despite not having any agreements on the books) have also been supportive of free data flows

12 Samm Sacks and Graham Webster, "Five Big Questions Raised by China's Cross Border Security Regulations," *DigiChina*, June 13, 2019, https://www.newamerica.org/cybersecurity-initiative/digichina/blog/five-big-questions-raised-chinas-new-draft-cross-border-data-ruless/

13 https://www.hawley.senate.gov/sen-hawley-chair-subcommittee-hearing-tech-companies-putting-consumer-data-risk-china-and-other

14 Laurens Cerulus, "Europe Eyes Privacy Clampdown on China," *Politico,* February 4, 2019, https://www.politico.eu/article/european-union-eyes-privacy-clampdown-on-china-surveillance-huawei/

15 Thank you to Nigel Cory for providing a definition of legal nexus.

16 Dr. Clarisse Girot (Project Lead and Editor), Regulation of Cross-Border Transfers of Personal Data in Asia (ABLI Legal Convergence Series: 2018).

17 See her tweet: Daphne Keller, October 23, 2019, https://twitter.com/daphnehk/status/1187077388925952001 This was specifically in relation to an Indian court decision ordering platforms like Facebook to take down information globally should Indian laws require it.

18 This is akin to internet governance questions of how much 'cyber sovereignty' is too much cyber sovereignty—i.e., as more countries exert greater sovereignty over the internet within their geographic borders, ranging from regulations on data flows to filtering network traffic for cybersecurity threats, what practices should and should not be considered acceptable by liberal democracies? See: Justin Sherman, "How Much Cyber Sovereignty is Too Much Cyber Sovereignty?," Council on Foreign Relations, October 30, 2019, https://www.cfr.org/blog/how-much-cyber-sovereignty-too-much-cyber-sovereignty

19 Nigel Cory, Robert D. Atkinson, and Daniel Castro, "Principles and Policies for 'Data Free Flow With Trust,'" Information Technology & Innovation Foundation, May 27, 2019, https://itif.org/publications/2019/05/27/principles-and-policies-data-free-flow-trust

20 For instance, countries that tightly restrict online content are also typically those that tightly restrict information in offline spaces, such as in public squares or in print media.

NEW AMERICA

This report carries a Creative Commons Attribution 4.0 International license, which permits re-use of New America content when proper attribution is provided. This means you are free to share and adapt New America's work, or include our content in derivative works, under the following conditions:

• **Attribution.** You must give appropriate credit, provide a link to the license, and indicate if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use.

For the full legal code of this Creative Commons license, please visit **creativecommons.org**.

If you have any questions about citing or reusing New America content, please visit **www.newamerica.org**.

All photos in this report are supplied by, and licensed to, **shutterstock.com** unless otherwise stated. Photos from federal government sources are used under section 105 of the Copyright Act.