

White Paper

Data Localization and Barriers to Cross-Border Data Flows Towards a Multitrack Approach

January 2018



White Paper Author:

William Drake

Contents

3	Executive Summary
4	Introduction
5	The Problems in Brief
7	International Trade Policy Responses
10	Guiding Principles and Objectives
12	Track 1: Nonbinding Intergovernmental Processes
14	Track 2: Multistakeholder Processes
16	Track 3: Digital Trade Processes
18	Conclusion
18	Acknowledgements
19	Endnotes

Executive Summary

Concern is growing about the data-localization requirements and barriers to cross-border data flows (CBDF) that have been established in a number of national economies, and that the trend could spread in the absence of well-structured and evidence-based international engagement. Concerted effort will be needed to get the balance right to avoid overly restrictive policies. Sustained public-private cooperation will be needed to move towards a more positive result.

Efforts to address these issues via international trade diplomacy have yielded mixed results. The World Trade Organization's (WTO) General Agreement on Trade in Services (GATS) is, arguably, applicable, but this has not been fully tested in the dispute resolution system and efforts to advance discussion of new and more specific disciplines are uncertain, at least the near term. The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) is set to contain more specific disciplines. However, these are accompanied by exceptions for legitimate public policy purposes that could create a large hole in the event of eventual implementation. Other trade deals that have been expected to contain similar provisions face varying levels of opposition and uncertain futures.

Part of the problem confronting trade agreements is that concerns about national sovereignty and jurisdiction, privacy and data protection, access to data and vulnerability to disruptions and so on can make the issues appear too multidimensional to agree binding trade commitments in the near term. At the same time, many internet stakeholders have evinced scepticism and even hostility about the prospect of "secret trade talks" serving as an important source of global internet governance – even if the two communities' objectives may be close in practice. There is a risk that their expertise and support for an open internet will be squandered and that some will oppose trade solutions.

To contribute to the dialogue on possible ways forward, this paper outlines three parallel tracks of international cooperation that could promote collective learning, shared understandings, and greater interoperability, convergence and ultimately regulatory coherence of policies on data localization and information flows among interested countries. The first track would consist of leveraging legally non-binding intergovernmental processes, e.g. "soft law" and "informal" agreements, transgovernmental networks, capacity building and knowledge-sharing arrangements, and the like – to institutionalize norms, the implementation of which could be monitored and reported on to encourage compliance. The second track would consist of multistakeholder processes and involve both expert-level work and broader public outreach and input to advance analysis, dialogue and mutual understanding on the issues. This would require networked forms of collaboration. The third track would involve enhanced international trade policy practices that are more transparent and open to diverse inputs, and which could ultimately lead to appropriate regimes such as a plurilateral digital trade agreement among willing partners.

The Forum has convened a series of multistakeholder dialogues exploring the overall topic and the multitrack approach to solicit feedback from a diverse group of experts. Based on those conversations as well as discussions in international venues such as the Internet Governance Forum, and building on an ongoing programme of work, the Forum will launch a public-private cooperation process drawing from several of the options laid out in this paper.

Introduction

This white paper lays out a set of policy options that the international community may wish to consider in order to build greater consensus on data localization and CBDF issues, which currently face uncertain prospects in the international trade policy context. It is not a report of research findings; a significantly longer and more detailed companion white paper will be released that summarizes the historical evolution of the policy debate, unpacks the individual issues raised by data localization and CBDF barriers, reviews the progress to date in international trade negotiations, advances a case for pursuing a multitrack approach to dialogue and consensus building, and then lays out possible options for action on three tracks of international cooperation in a manner as outlined in the contents of this paper. As such, this paper should be viewed as part of a larger research effort and as one that simply splits out the policy options to facilitate action-oriented discussions in the immediate future by decision makers and influencers.

The Problems in Brief

Data flows have become the lifeblood of the global digital economy, and the internet and other electronic networks are its circulatory system. As McKinsey estimates, total cross-border internet traffic increased eighteenfold from 2005 to 2012¹, and “data flows account for \$2.8 trillion of global GDP in 2014 and “cross-border data flows now generate more economic value than traditional flows of traded goods”. The new business models and markets that will increasingly drive the Fourth Industrial Revolution² and the world economy in the years ahead are predicated on the ability of data to move as seamlessly as possible across a reasonably open and unfragmented internet. With the spread of artificial intelligence and robotics, data flows will give rise to entirely new methods of production, process and relationship management and consumption. Importantly, CBDF empower not only large multidivisional and geographically dispersed firms but also micro, small and medium-sized enterprises (MSMEs) that can access global markets in ways that were previously unimaginable³. And while much of the discussion on the importance of CBDF and related trends has centred on business concerns, it must be underscored that there are profound implications for our ability to address global challenges and deliver sustainable development⁴.

Yet despite the many benefits of open data flows, a growing number of governments around the world have enacted policies compelling various forms of data localization and erecting barriers to CBDF. These are not new phenomena. Many policy-makers have long maintained requirements that certain classes of sensitive information (e.g. pertaining to national security, law enforcement, and financial matters) be retained in-country and processed by firms of national origin. But the incidence and breadth of such policies have significantly increased in the past few years and there is a risk that restrictive approaches could spread more broadly.

Surveys of impacted businesses have provided useful evidence. In 2014, the US International Trade Commission produced a report based on responses from over 3,600 firms to a questionnaire indicating that, “Eighty-two percent of large firms and 52% of [small and medium-sized firms] in the digital communications sector felt that localization requirements presented obstacles.”⁵ Other studies by governmental bodies and think tanks have provided broadly similar upwardly mobile indicators, although the data’s comparability is often limited by methodological and related factors.

The most common form of data localization appears to be a requirement that data be locally stored or “resident” within a country. Sometimes this is complemented by a requirement that data be processed by entities physically within a national jurisdiction, or even that such processing must be carried out by national firms or at least involve a specific level of “local content” in terms of services and equipment. Others forms of mandated localization could include requirements that processing and/or storage conform to unique national rather than internationally accepted technical and operational standards, or that data be routed largely or solely within a national or regional space when possible.

Some restrictions are borne from legitimate and important concerns related to privacy, security and banking prudential regulation. However, in whatever form they take, data localization policies can impose restrictions that are greater than what may be required to achieve legitimate national goals. Moreover, they can be self-defeating. From an economic standpoint, as Anupam Chander and Uyen P. Le point out: “Data localization raises costs for local businesses, reduces access to global services for consumers, hampers local start-ups and interferes with the use of the latest technological advances... Data localization, like most protectionist measures, leads only to small gains for a few local enterprises and workers, while causing significant harms spread across the entire economy. The domestic benefits of data localization go to the few owners and employees of data centres and the few companies servicing these centres locally.”⁶ MSMEs, both domestic and international, may be especially hard hit.⁷ Facing the complexity and high cost of operating redundant infrastructure and otherwise complying, firms that provide great value to local citizens may simply choose not to service a market, as recently happened with LinkedIn in Russia. In addition, some analysts argue that the evidence suggests that localization policies can have a notable negative effect on GDP.⁸

Similarly, from a human rights standpoint, some of the governments involved engage in significant levels of digital surveillance of their populations and applying data localization requirements may simply make their jobs easier. And localization is unlikely to greatly affect the operations of intelligence agencies. As one analyst summarizes: “The notion that data must be stored domestically to ensure that it remains secure and private is false. In regard to security, while certain laws may impose minimum security standards, the security of data does not depend on where it is stored, only on the measures used to store it securely.”⁹

Barriers to CBDF present different but sometimes interrelated challenges. Some studies have indicated that the most common objective of cross-border data transfer measures is to protect the privacy of data subjects. Closely related, and often based on similar arguments, are concerns relating to security.

CBDF barriers justified in terms of privacy and data protection may be tied to data-localization requirements. In contrast, the European Union's privacy policies, including the General Data Protection Regulation (GDPR) that comes into force in May 2018, are not designed to force local retention or processing in the name of techno-nationalist industrial policies or expansive notions of "cyber-sovereignty" and national security. If it can be determined that the countries to which personal data on Europeans would be transferred offer adequate or effectively comparable protection, then barriers are not required. In short, whether privacy or security is being invoked with potential protectionist intent varies across cases, which arguably raises issues about the application of trade and other international rules.

While some studies do not delve into the matter, others rightly treat censorship and related content controls as CBDF barriers as well.¹⁰ In its 2017 *Freedom on the Net* report, Freedom House examines 65 countries worldwide, accounting for 87% of the world's internet users. Only 13 countries were judged to have seen an increase in internet freedom from the previous year, while 32 saw a decline.¹¹ These findings are broadly consistent with other reports, and often the restrictions broadly frame prohibitions on accessing entire platforms and information ecosystems rather than just specific websites or kinds of information. Where content is blocked and filtered, data flows are as well. And, of course, there are many other sorts of policies that can impede data flows, such as those pertaining to encryption, liability, intellectual property and so on.

International Trade Policy Responses

Governments and firms concerned about these trends have been pushing for some time to redress them via international trade disciplines. At the broad multilateral level, the World Trade Organization's (WTO) General Agreement on Trade in Services (GATS) is, arguably, directly applicable to the issues at hand. During the 1986-1994 Uruguay Round negotiations that established the WTO, many countries made liberal commitments on computer and related services, which include data-processing services, database services, and others that can be said to correspond to many of today's internet services. Moreover, the US gambling case that was adjudicated in the WTO dispute settlement system determined that full market-access commitments on cross-border supply implies the right for other members' suppliers to supply a service through any means of delivery, including the internet. Accordingly, one could argue that "data localization measures violate existing GATS rules and commitments to allow unrestricted cross-border trade in digital services and cross-border data flows."¹² Similarly, "restrictive data transfer measures could breach the non-discrimination and market access disciplines under the GATS, except to the extent that they are justified under the general exception in GATS Article XIV."¹³ Other WTO rulings may also be relevant to the debate.¹⁴

Some stakeholders, however, believe that specific positive commitments on the services with respect to data localization and CBDF have not been made. Some also maintain that the general exceptions of Article XIV regarding national security, public morals and order and privacy protection provide sufficient leeway to undertake these policies. Accordingly, since no party to the agreement has been willing to press a claim in the dispute settlement system to test the GATS applicability, attention has focused for several years on the possibility of launching a new process that could lead to the negotiation of specific provisions concerning data localization, CBDF and related digital-trade issues.

The debates on these matters have featured in some WTO proposals but also have elicited push-back from key countries and regions. They maintain that any such discussion would be premature. A statement submitted by the African Group to the WTO's General Council in July 2017, for instance, stated that negotiations on digital trade could cement and widen the technology divide; deny governments' ability to use "smart industrial policy tools" or "powerful protectionist tools" like data localization requirements, internet filtering and technology transfer requirements (i.e. disclosure of source code) to promote domestic digital firms and allow them to catch up with the leading multinational firms. They could also lock in a situation where their citizens' data is being given away for free for the commercial benefit of the largest digital firms rather than being used for their own national economic advantage.¹⁵ A subsequent contribution in October 2017 maintained "the propaganda that new e-commerce rules will be

good for developing countries has been highly contested" and sharply questioned the assertion that existing WTO agreements and commitments apply to electronic commerce.¹⁶

Other developments have occurred through the WTO's regular committee work. In September 2017, the US circulated a communication in the WTO's Council on Trade in Services concerning China's new cybersecurity law, which inter alia entails expansive data localization and CBDF restrictions. The statement argued that: "China has undertaken market access and national treatment commitments under the GATS for many services that would be affected by these measures. In addition, China's cross-border commitments apply to a broad range of sectors – from accounting to financial data processing to travel services. None of these cross-border services is feasible without accessing data from China, much of which would appear to fall within the scope of the restricted or banned categories." As such, the US requested that China "refrain from issuing or implementing final measures until such concerns are addressed".¹⁷

The US submission was discussed in the Council on Trade in Services in October 2017. The Japanese delegation provided detailed comments expressing concerns about various aspects of the Chinese law and the EU raised related concerns. The US summarized that the law "could disrupt, deter and, in many cases, prohibit cross-border transfers of information that were routine in the ordinary course of business" and that the "impact of the measures would fall disproportionately on foreign-service suppliers, which obviously had a greater need to communicate internationally than domestic firms because they either needed to transfer data to and from headquarters and other affiliates or, in the case of cross-border supply, to interact with customers located in China."¹⁸ Similar concerns were expressed about Viet Nam's draft cybersecurity law.

It is far too early to guess where this discussion will lead, and especially whether the US or other WTO Members could ultimately choose to engage the organization's dispute settlement system in such a sensitive circumstance. Nevertheless, it does seem that serious consultations could ensue over the nature of the existing GATS rules and national commitments, including with respect to national treatment.

Some countries have pursued the inclusion of bespoke language on data localization and CBDF in a variety of bilateral, regional and mega-regional free trade agreements. For example, the US and Republic of Korea free trade agreement, which came into force in 2012 (and which the Trump Administration now says it wants to renegotiate) calls on parties "to endeavor" to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders. Far more exacting was the detailed

language included in the Trans-Pacific Partnership (TPP) deal signed in February 2016. The TPP contained among its many provisions elaborate articles on personal information protection, cross-border transfer of information by electronic means, and location of computing facilities that set out the clearest binding disciplines yet on localization and CBDF restrictions. In both cases, language adapted from GATS Article XIV specified that governments could maintain measures to achieve legitimate public policy objectives provided these are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and do not impose restrictions greater than what is required to achieve the objective in question.¹⁹

The TPP language was hailed by trade proponents and is reported to be on the table in the ongoing renegotiation of the North American Free Trade Agreement (NAFTA). Moreover, similar language reportedly has been proposed for the Transatlantic Trade and Investment Partnership (TTIP) and the Trade in Services Agreement (TiSA). However, the former is off the table and the latter is in a major holding pattern. The NAFTA talks also seem to be facing significant hurdles. In addition, the Trump Administration has pulled out of the TPP, leaving the other 11 members to push forward with a revised Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). In short, save for among the remaining CPTPP partners, trade agreements alone seem unlikely to provide a near-term solution to the problems of data localization and CBDF barriers.

Moreover, the challenges to digital trade agreements are not only intergovernmental. For example, there is a good deal of mistrust among many denizens of the 24/7 globalized infosphere who fear that “secret trade deals” will be made that could curtail their freedom to create, access and disseminate information. Such sentiments are by no means limited to the sort of anti-globalization civil society activists that are familiar to trade policy-makers. It is also evident to varying degrees among the wide array of people and organizations active in the multistakeholder internet governance community. They include not only civil society actors but also the internet technical community that designs and operates significant portions of internet infrastructure and applications, and even entrepreneurs and business people who are acclimatized to the habits and mindsets prevalent in these arenas. The models of decision-making they embrace are based on total transparency, peer-to-peer bottom-up community participation that is open to all, and consensual decision-making.

Consider, for example, the Brussels Declaration on Trade and the Internet released in March 2016:

“We are an expert group of stakeholders representing internet users, consumers, innovative businesses, cultural institutions and scholars. We recognize the considerable social and economic benefits that could flow from an international trading system that is fair, sustainable, democratic and accountable. These goals can only be achieved through processes that ensure effective public participation. Modern trade agreements are negotiated in closed, opaque and unaccountable fora that lack

democratic safeguards and are vulnerable to undue influence. These are not simply issues of principle; the secrecy prevents negotiators from having access to all points of view and excludes many stakeholders with demonstrable expertise that would be valuable to the negotiators. This is particularly notable in relation to issues that have impacts on the online and digital environment, which have been increasingly subsumed into trade agreements over the past two decades.

The procedural deficits that define modern trade-agreement negotiations have resulted in instruments that are unduly deferential to the interests of a narrow class of established industry stakeholders and fail to address the needs of broader affected communities. This stands in stark contrast to the more open internet governance process norms to which the governments that negotiate trade agreements also notionally subscribe, which, if fully realized, would be better adapted to incorporate the values of these communities, such as free expression and cultural facilitation, into trade policies. Any international rulemaking process that affects the online and digital environment should adhere to human rights and good governance obligations to actively disseminate information, promote public participation and provide access to justice in governmental decision-making.”²⁰

Signatories to this statement included such entities as the American Library Association, the Association of College and Research Libraries, the Association of Research Libraries, the International Federation of Library Associations and Institutions, Creative Commons, European Digital Rights, and the Mozilla Foundation. Moreover, the i2Coalition, although not a signatory to the document, declared that it supports many of the declaration’s broad goals, adding that it “participated in the discussions ... because of our deep belief that many voices are not being heard when discussions about trade and the internet intersect. It is our opinion that the serious consideration of diverse views will lead to better trade agreements.”²¹ This coalition comprises over 80 internet businesses, including service providers and leading players in the domain name and related sectors like VeriSign, GoDaddy, Affilias and Google.

In a similar vein, the Global Commission on Internet Governance, chaired by Carl Bildt (Swedish Prime Minister 1991-1994), released a report, *One Internet*, at the OECD’s Ministerial Meeting on the Digital Economy at Cancún in June 2016. The report noted that:

“... bilateral and multilateral free-trade agreements can significantly affect internet governance issues. Many, such as the Trans-Pacific Partnership Agreement, specifically address important issues such as data localization, encryption, censorship and transparency, all of which are generally regarded as forming part of the internet governance landscape. However, they are negotiated exclusively by governments and usually in secret ... The fact that these negotiations are open only to governments has inspired protests by non-governmental actors demanding that they be informed and engaged in negotiations to allay fears that the new rules embedded in these agreements

favour the interests of governments or corporations over those of other internet users. The closed nature of the negotiations also means that the benefits governments hope to achieve may not be evident to the general public.”²²

If and when the machinery of international trade policy deepens its engagement with internet-related questions like data localization and CBDF barriers, it is entirely possible that support among organized internet stakeholders will be thin. There also could be significant opposition. In particular, certain stakeholders believe that any digital trade deals will undermine privacy and data protection, result in overly restrictive intellectual property protections and generally favour the interests of large organizations over global public interest.

With all this in mind, the time is ripe to consider a multitrack approach to promote collective learning and shared understandings – between policy communities as much as the governments that house these – and greater interoperability, regulatory cooperation and, ultimately, coherence of policies on data localization and CBDF.

Guiding Principles and Objectives

In recent years, many international meetings and associations have proposed guiding principles for global internet governance that could be helpful in charting a way forward on data localization and CBDF issues. Arguably, of particular interest are the principles agreed to at the NETmundial Global Multistakeholder Meeting on the Future of Internet Governance held in São Paulo in April 2014. Representatives from governments, the private sector, the internet technical community, civil society and academia signed off a “roadmap for the future” as well as two sets of principles. The first pertained to substantive objectives and included:

- Human rights/shared values (freedom of expression and association, freedom of information, access to information, privacy, accessibility and development)
- Protection of intermediaries
- Cultural and linguistic diversity
- Unified and unfragmented space
- Security, stability and resiliency of the internet
- Open and distributed architecture
- Open standards
- Enabling environment for sustainable innovation and creativity
- Access and low barriers

The second pertained to the conduct of internet governance and included that processes should be:

- Multistakeholder
- Open, participative, consensus-driven governance
- Transparent
- Accountable
- Inclusive and equitable
- Distributed
- Collaborative
- Enabling meaningful participation
- Agility²³

In addition, other principles that could be customized to this initiative may include:

1. Put the internet first. Evidence suggests that proponents of restrictions sometimes view the issues as revolving around the preferences, actions and relative positions of particular countries and companies. This orientation can lead to self-defeating policies that are deleterious not only to the countries involved but also to the global internet. Accordingly, it would be useful to reframe the policy discourse to emphasize the importance of avoiding undue fragmentation of the internet and preserving its integrity, openness, end-to-end interoperability, generativity and long-term value as a flexibly redeployable pool or resources and functionalities to all actors and the world economy as a whole.

Such a discursive turn, framed in terms of the global public interest, also would be likely to garner more widespread political support from diverse actors who are more concerned with advancing systemic rather than particular interests. It could also help to assuage the concerns of some about internet openness being cast as another bargaining chip to be offered or withheld in the context of single trade undertakings involving a range of other issues.

2. Focus on jurisdiction over and access to data rather than its physical location. The notion that the physical location of data is the key to ensuring the achievement of national policy objectives belies the very nature of the internet. Any piece of online data simultaneously may be stored in caches, distributed, copied, backed up and used to derive other data in multiple machines in multiple countries.²⁴ The ephemeral and transitory nature of data in a globally interoperable network of over 60,000 autonomous systems has given rise to a raging debate among legal scholars as to the relationships between data and territoriality and the use of extraterritorial claims of jurisdiction.²⁵

It seems possible that policies based on assigning a geographical fixity to data could prove to be as legally unsustainable as they are operationally ineffective. At the same time, technologies and procedures for authentication, monitoring and auditing could help to assure that data held abroad is sufficiently accessible and secure. Hence it might be better to refocus international debate on agreeing principles for determining effective jurisdiction (including in cases of multiple competing claims) and providing governments and other actors with responsive access when needed.

3. Emphasize the diversity of stakeholders impacted by restrictions. In parallel, the policy discourse must emphasize that the issues are not principally about regulating a small number of large technology suppliers and platform operators, but rather about how restrictions impact everyone in every sector of the economy and society that are dependent on the internet and related systems and services. MSMEs on the supply side of the market, as well as customers large and small from across every sector of the economy, may suffer from excessive obligations and restricted choices. The same can be said of non-commercial organizations, individual users and even the public sector.

In particular, it would make sense to emphasize the “right of the consumer” to access and disseminate data and information via electronic networks or any other medium irrespective of geographical location. This would be consistent inter alia with the Universal Declaration of Human Rights, as well as with the Estonian government’s proposal that the free movement of data should be regarded as a Fifth Freedom under EU law.

4. Engage with the concerns driving restrictive policies.

In the past few years, industry associations, consultancies, think tanks and government agencies in developed economies, particularly in the US, have produced a bevy of reports and statements arguing that data localization and CBDF barriers are a threat to the world economy. Many of the reports follow a similar trajectory. For example, they assemble evidence of the trends (often citing the same set of national cases about which there is clear information); briefly cover some of the possible rationales for restrictive policies and state why they are wrong; and then argue that international policy harmonization is urgently needed, typically via international trade agreements. Usually, at least to the present author's knowledge, they are written in English and build their cases by citing each other, since they constitute the available literature.

What we are missing thus far is a truly international, multistakeholder and multidisciplinary discussion of the issues. Such a discussion should include and seriously engage with the views of the governments, stakeholders and analysts that favour government activism on digital issues, even including restrictive policies. In the absence of this discussion, the critics of such measures are preaching to their choir while actors with different views are left frustrated and may drive the issues into organizational settings – e.g. the Collective Security Treaty Organization, Shanghai Cooperation Organization, the BRICs – where statist views on internet matters are the common denominator.

A significant number of countries are not prepared to contemplate negotiations that ultimately could include the sorts of limitations on data localization and CBDF barriers that have been proposed in the various PTAs and adopted in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP). Indeed, a significant strain of thinking points in an opposite, somewhat techno-nationalist direction. Arguably, the best way to deal with such views and move to shared understandings and preferences is via open dialogue; and to do that we need to construct the institutional settings in which it can occur.

5. Draw from the full menu of global governance models.

As mentioned above, the default assumption of the growing body of reports, industry statements and Western government statements on data localization and flows has been that new trade disciplines are urgently needed. This approach has obvious appeal since trade agreements are legally binding and have mechanisms for dispute resolution and the sanctioning of non-compliance. However, it is clear that many countries, especially those that have adopted or considered restrictive measures, simply are not ready to sign up to such solutions in the near term. Arguably, it would hence make sense to pursue alternatives to promote collective procedural and substantive learning and a more widely shared understanding of the issues and implications of alternative approaches. This could ultimately make trade deals easier to achieve further ahead and, before then, provide a greater measure of international ordering and predictability than we have at present.

In this context, it would make sense to recall the larger direction of movement in global governance over the past years. The governance tool set has expanded significantly, with “soft law” and informal instruments, transgovernmental and transnational policy networks and multistakeholder processes playing increasingly central roles in problem-solving.²⁶ In some cases, such approaches have been found to be reasonably sufficient on their own in encouraging/nudging movement towards shared approaches. In other cases, “hard agreements” have incorporated soft or informal elements within their terms, as per the KORUS provision calling on parties “to endeavour” to refrain from imposing or maintaining unnecessary barriers to CBDF. Similarly, the WTO has become an umbrella for mechanisms oriented more towards capacity-building such as the Aid for Trade Initiative.²⁷ In still other cases, such nonbinding mechanisms have been deployed alongside binding instruments, resulting in an evolutionary manner in hybrid “regime complexes” of interrelated and mutually reinforcing injunctions.²⁸ With all this in mind, the multitrack approach outlined here comprises policy options that collectively or in part could help foster near-term collective problem-solving on data localization and CBDF.

While these options are presented as an interrelated set that could serve as the framework for a multitrack initiative combining intergovernmental and multistakeholder workstreams, they also may be seen as being modular. This reflects the reality that even an initiative concentrating on just these two complex issues could prove to be more ambitious and demanding than what can get buy-in and be sustained by the range of organizations whose involvement would be necessary. Should this prove to be the case, a few of the options could be selected and pursued instead. Progress on a subset of options could provide a baseline from which the pursuit of work on others might get political traction. There has been no shortage of grand plans to deal with internet policy issues that looked good on paper but have not been followed up on in practice, so caution and consideration of “plan B” approaches is of course advisable. It is also important to consider the governance levers and implementation processes to encourage movement from principles to concrete actions generating measurable results.

Track 1: Nonbinding Intergovernmental Processes

The first track of activity could involve making fuller use of existing nonbinding intergovernmental processes. Debating the issues and developing legally nonbinding agreements free from the immediate pressures of trade negotiations could advance the trust and mutual understanding needed to discourage overly restrictive approaches, encourage early adopters of restrictions to contemplate some softening, and perhaps even lay the groundwork for binding commitments that best deliver on desired economic and social objectives.

1. Pursue greater precision at the G7 and G20 meetings.

The G7 Summit 2016 declared its support for “ICT policies that preserve the global nature of the internet, promote the flow of information across borders” and also its opposition to “data-localization requirements that are unjustifiable taking into account legitimate public policy objectives.”²⁹ Although it sidestepped data localization, the G20 Summit 2016 expressed support for “policies that preserve the global nature of the internet, promote the flow of information across borders and allow internet users to lawfully access online information, knowledge and services of their choice. At the same time, the G20 recognizes that applicable frameworks for privacy and personal data protection, as well as intellectual property rights, have to be respected as they are essential to strengthening confidence and trust in the digital economy.”³⁰ The G20 ministerial declaration did reiterate the previous year’s formulation on CBDF.

Might it be possible to revisit these formulations and attempt to increase their precision? When the G7 speaks of localization, what kinds of measures are considered to be (un)justifiable in terms of legitimate public policy objectives? When the G7 endorses “the flow of information across borders”, does this mean the free flow, and, if not, what qualifications apply? How exactly does this relate to respecting applicable frameworks for privacy and personal data protection? More precise language might prove difficult to reach but the process of discussing it could be useful. Formal organizations could take up the issues in parallel and provide inputs, and stakeholders could be usefully engaged both in the summit mechanisms and elsewhere, as suggested below.

2. Delegate to institutionalize an agenda. The G7 and G20 do not have an overarching organizational machinery and continuity to carry forward the streams of ancillary work that would be needed to progress data localization and CBDF issues or to address the related concerns that have animated regulatory responses. However, if progress could be made at senior governmental meetings in more tightly bounding the issues and establishing a political mandate, the responsibility for fleshing out and encouraging implementation of the rules could be allocated to actors that have the requisite capacity. This could be done at several levels: e.g. intergovernmental organizations, networked national agencies and multistakeholder organizations. Staff and resources could be mobilized or reallocated to embed

the issues in their respective agendas as focal points for ongoing monitoring, analysis and action, as well as to facilitate outreach to wider publics. Some possible avenues for such a build-out follow.

3. Orchestrate coordination between intergovernmental and multistakeholder processes. In its report for the G20 2017 process, the B20 business alliance suggests one such path toward collective action:

“The G20 should ask UNCTAD and the OECD to facilitate and guide an inclusive dialogue towards consensus-building among all G20 members on interoperable standards for non-personal data protection as well as privacy protection. Senior experts of private and public organizations should be involved in the dialogue to ensure a holistic view on this topic. As a starting point, UNCTAD and OECD should use the results of the work with relevant stakeholders at the OECD on cross-border data flows, which was initiated as a follow-up to the OECD Ministerial Meeting in Cancún. Furthermore, UNCTAD and OECD should develop an interoperable framework of guiding principles on policies related to cross-border data flows with the involvement of senior experts of private and public organizations, which – respecting the right of governments to regulate where necessary and appropriate – can be adapted by countries. The principles should incorporate a holistic approach that ensures cybersecurity, data and privacy protection, and free and trustworthy cross-border data flows in a way that reflects the needs of international business solutions and supply chains... To foster legal certainty and transparency related to cross-border data transfer or storage, UNCTAD and OECD should – together with G20 members and above-mentioned senior experts – propose a set of global guiding principles that clarify which jurisdiction applies under which circumstances.”³¹

This is a network model that positions two key intergovernmental organizations as its lead nodes. Both have significant technical expertise and organizational capacity, their memberships cover governments of the global North and South, and they have working relationships with some of the more focused and active stakeholders in their respective areas of work. Nevertheless, it might not be optimal to have two intergovernmental organizations as the sole leads for ambitious initiatives that would require wider multistakeholder engagement and a sense of ownership, as well as transparency and a measure of inclusion in relation to wider global publics.

It could be sensible to enlist as lead partners a few multistakeholder organizations such as the World Economic Forum, the Internet Society, and even one of the internet governance civil society coalitions. The staff or secretariats could coordinate among themselves and then “orchestrate” the structured engagement of perhaps concentric circles of public and private partners.³² Such orchestration can be

demanding but is needed to ensure that relevant experts can collaborate intensively while others are able to provide inputs and track developments to ensure legitimacy and accountability.

4. Promote transgovernmental regulatory cooperation.

Transgovernmental networks are playing increasing roles in many domains of global governance. The E15 project offered a number of good suggestions on this score, arguing that national regulators should build out working relations on a number of key aspects of digital trade such as privacy protection.

Growing interoperability between the US-EU Privacy Shield, the EU GDPR, the OECD guidelines, the APEC's Cross Border Privacy Rules (CBPR) and other ordering techniques, binding corporate rules and other approaches is a widely recognized priority. As UNCTAD has noted: "While there exists a remarkable degree of harmonization and coherence around the data protection core principles in international and regional agreements and guidelines, there are diverging implementation practices."³³ National agencies are best placed to catalogue, compare and seek to reconcile those practices. Moreover, should such collaboration lay the groundwork for a more expansive effort, the engagement of national agencies would be crucial here too. As the OECD has noted: "The current patchwork approach to privacy and data protection and to digital security across the G20 creates frictions in a data-driven global economy... Targets could include fostering international arrangements that promote effective privacy and data protection across jurisdictions, including through the development of model privacy strategies."³⁴ Indeed, some in the private sector even consider that "there is a clear need to work with all data-protection agencies on an *international data transfer regime*, that guarantees the effective protection of privacy at an international level as well as to ease the international flow of personal data, essential in a globalized world."³⁵

The E15 also took note of the potential role of consumer protection agencies. "Cooperation among consumer protection agencies can help increase consumer protection for digital trade and thus raise confidence and willingness to engage in such trade."³⁶ Fully engaging consumer agencies could prove to be vital, especially if we were to take up the above-mentioned idea of a "right of the consumer" to access and disseminate data and information via electronic networks or any other medium irrespective of geographical location. This could be a useful principle to feed back up the organizational chain as part of a larger complex of legally nonbinding but strongly encouraged complex of international prescriptions.

5. Establish monitoring and reporting mechanisms to enhance the sense of obligation and encourage compliance with shared norms and good practices.

To make legally nonbinding agreements worth more than the paper they are written on, it is imperative to establish mechanisms through which data on the conformity of national practices with international agreements is systematically tracked, aggregated and publicly reported in a manner that facilitates easy and accurate comparative assessments of progress. Civil society groups sometimes refer to this technique as "naming and shaming" but the function should not be cast in an adversarial manner that could elicit bureaucratic wagon-circling and creative reporting. Experience in other arenas demonstrates that when national performances are arrayed next to each other, and especially if they are ranked on some measures of attainment, governments and other organizations may feel normative and reputational pressures to "up their game". In some cases, it could be sensible to delegate responsibility not only to international organizations and national agencies but also to duly accredited stakeholder groups that are "on the ground" and able to report on their lived experiences with localization and CBDF barriers.

Establishing monitoring and reporting mechanisms also would help with one of the overarching challenges that confound all efforts to assess this policy arena, namely the lack of solid, up-to-date, comparable data on localization and CBDF barriers. There have been various efforts by governments, industry associations, think tanks and intergovernmental organizations to assemble hard data, often via surveys, but these typically are too patchy and variable to provide a consistent and reliable picture of the state of play. Mobilizing a decentralized effort by trusted partners could help to fill this rather debilitating gap.

6. Launch capacity development efforts. Governments in developing and transitional countries will benefit from engaging technology experts, stakeholders and development specialists about the operational and other consequences of localization policies and CBDF barriers, as well as alternative ways to cultivate local digital activities to enhance national prospects. Some stakeholders would need support to master the issues and then engage and contribute effectively. A wide variety of programmes is already under way – both top-down governmental/ intergovernmental and, more interestingly, bottom-up and driven by the internet community – that are training thousands of people a year on internet governance and related issues. Perhaps some of these could be used to add data localization and flow issues to their programmes.

Track 2: Multistakeholder Processes

The second track of activity would involve drawing in the robust and well-institutionalized communities of technical experts, industry representatives and civil society organizations and individuals that are deeply engaged on internet governance and policy matters. Many of these actors are accustomed to working through multistakeholder decision-making processes in bodies such as the Internet Engineering Task Force, the Regional Internet Registries, the Internet Corporation for Assigned Names and Numbers, and the Internet Governance Forum and its various offshoots. The models of decision-making they embrace and expect are based on strong transparency requirements; peer-to-peer, bottom-up community participation that is open to all; a sense of ownership of the processes they have laboured to develop and, in many cases, decision-making by consensus or rough consensus.

The participation of internet stakeholders would strengthen the knowledge base needed to address the issues and could ensure that any results of policy processes have broadened support. The multitrack approach outlined here opens up these possibilities in a way that the status quo trade-centric trajectory does not. Of course, organizing new multistakeholder processes that are not centred on engaging with an existing process, such as those mentioned above, can be fraught with complexities. Inevitably, there could be some lively debates about who gets a seat at which table through what mechanisms, and whether those seated are sufficiently representative of the wider communities etc.

In particular, issues could arise among those civil society coalitions that tend towards anti-globalist views and are highly critical of what they see as concentrated corporate power. Such groups, however, tend to be much more prominent in trade than internet governance, where the dominant orientation is favourably inclined towards multistakeholder processes in which collaboration with the private sector is routine. As such, the challenges of managing an open process ought to be manageable, especially if there is deft and transparent orchestration by the “lead hub” organizations of a new policy network. With these considerations in mind, we might consider the following policy options for this track of activity:

1. Facilitate the development of a multistakeholder and interdisciplinary community of expertise and practice.

As noted previously, the global dialogue on localization and CBDF has not been characterized by broad and diverse engagement and only a few of the internet experts with significant technical and policy expertise appear to be closely engaged on the issues. Nevertheless, the growing buzz around digital trade generally provides an opportunity to promote greater focus and the progressive coalescing of a community of stakeholders that recognizes the importance of these issues and the opportunity to tackle them. The organizations mentioned above as possible lead nodes in

an emergent policy network could play a role in catalysing this process, especially by emphasizing the risks of internet fragmentation.

2. Establish a multistakeholder expert grouping that can be a focal point of contact for intergovernmental processes and produce its own outputs.

The lead node organizations mentioned above could use their convening powers to put out an open call for a group comprising a balance of stakeholders with demonstrable expertise on relevant issues. The stakeholders could organize their own bottom-up processes to put forward names, and the assembled group could define the modalities of its work and the means by which it would invite inputs from and be accountable to the wider communities. There would then be a “peak group” to whom the conveners could turn to promote direct multistakeholder participation in the Track 1 activities, in accordance with the applicable respective rules of engagement. In addition to providing an interface with intergovernmental discussions, such a group could undertake its own parallel work programme to generate various kinds of output.

One could imagine a multistakeholder expert group that could produce a report that delved into the issues in a way that would be difficult for an international organization to release under its own name. For example, undeniably important issues and developments that might be objected to by an international organization’s member governments could be discussed openly, as could broader questions concerning “data-fication”, the platform economy and so on that have figured in the thinking of some proponents of localization and barriers. In this way, a report could serve to release pressures that might otherwise burst out of other less-balanced venues. At the same time, having a global research network generate detailed issue papers would help to institutionalize the issues on the agendas of various actors and promote the coalescence of the above-mentioned community of expertise and practice. All such products could be provided as inputs into intergovernmental deliberations, both within the nonbinding processes of Track 1 and the trade policy processes of Track 3, below.

3. Create parallel mechanisms to promote broader public engagement and input.

It would not be enough to create a multistakeholder expert group and stop there. Some parties who are not able to join the group might regard it as a closed, “elite” process, especially if it were to operate under the Chatham House Rule or other limitations on transparency. To benefit from a wider range of viewpoint and be viewed as legitimate, an expert grouping would need to be complemented by mechanisms facilitating wider public engagement.

Existing open processes could be leveraged to promote this transparency and engagement. For example, open face-to-face meetings with remote participation could perhaps

be held in the context of the annual UNCTAD E-Commerce Week. The annual global Internet Governance Forum, and the various national and regional meetings that have spun out of it, could provide other opportunities for broader debate. As of 2017, a new multistakeholder Dynamic Coalition on Digital Trade is working to bring issues such as data localization and CBDF to the attention of the internet governance communities.

4. Conduct expert analysis and dialogue on trade exceptions provisions.

A good starting point for multistakeholder discussions would be to “open up” these key trade concepts for consideration and debate.

It could be very useful to engage stakeholders in an assessment of these issues. On the one hand, some could bring to the discussion significant business and technical expertise that would be helpful in considering what kinds of measures truly are arbitrary and greater than what is required to meet the declared objectives. On the other hand, some stakeholders worry that these provisions open the door to dispute resolution cases that could result in decisions that do not take into consideration the full range of societal interests at stake; for example, with respect to privacy and data protection. An expert-level assessment supplemented by broader public input could help to build consensus on the utility and proper scope of the exceptions criteria and hence make their use more widely supported.

Track 3: Digital Trade Processes

The third track of activity would consist of work undertaken in intergovernmental trade policy settings. Current efforts to bring forced data localization and CBDF barriers more explicitly under international trade disciplines could be recalibrated to allow some alignment with this multitrack architecture. This would effectively mean nesting existing and new trade disciplines of relevance in a broader regime complex of mutually reinforcing discussions and instruments.

Any measure of consensus and convergence achieved on Tracks 1 and 2 could then be considered by the participants in Track 3 as they continue their work in accordance with their own work programmes. In parallel, stakeholders would be able to participate in the wider process in ways that might ultimately enhance their support for internet-related international trade policies. With these considerations in mind, we might consider the following policy options for this track of activity:

1. Clarify the applicability of existing GATS disciplines and related national commitments. Analysis and dialogue on this issue might usefully be undertaken by an expert multistakeholder configuration as discussed above with an eye to providing a supportive input to the trade community. Clearly, however, a parallel and more authoritative discussion needs to happen among WTO negotiators as well.

2. Carefully consider which issues really need to be addressed via trade disciplines. Here too, parallel discussions within and outside formal trade policy settings would be useful. If one assumes by default that trade agreements are “the only game in town” for bringing international order to the policy space, then there may be a temptation to load into them provisions on digital issues that might be more easily addressed via other international mechanisms. Whether digital trade rules should be broadly scoped or narrowly tailored is a matter of some controversy among governments and internet stakeholders alike.

For example, a recent working paper by the European Parliament’s Committee on International Trade argues that “...rules on the processing of personal data should not, are not and will not be a part of trade negotiations. The EU’s General Data Protection Regulation *acquis* shall not be undermined by trade agreements, which is a position that has been repeatedly reiterated by all European institutions... [and] ...while international cooperation is key to combat counterfeiting, trade agreements are not the place to extend the level of protection for rights holders by providing for more extensive copyright enforcement powers.”³⁷ At the same time, the committee argues that trade agreements should ban forced data localization, prohibit the forced disclosure of source code, limit intermediary liability and promote the use of encryption and the adoption of net neutrality policies. Other actors have advanced different lists

of issues they regard to be in or out of scope for potential new rules. Views on this may impact solutions regarding data localization and flows.

There are further practical limitations to a trade discipline approach. Even in the best environment, trade agreements take several years for political agreement, legal scrubbing and implementation. More time would then be needed to litigate any potential disputes. Because the pace of technological change is moving so rapidly, it is highly likely that inefficient networks will be locked in for many years before any positive movement from trade efforts.

3. Clarify the relationship between privacy and data protection and international trade disciplines. The fear, particularly in Europe, that trade mechanisms could be used to gut the protection of fundamental human rights has had a significant negative impact on the politics and public perceptions of data localization and CBDF proposals. It has in parallel greatly complicated trade negotiation processes; for example, in TiSA and JEEPA, where the EU has struggled to come to a common position blending the free flow of data with privacy protection. As long as European Parliament members and the broad range of internet stakeholders that prioritize privacy believe that trade disciplines constitute an existential threat, support for strong language on data localization and CBDF will remain unduly shallow.

4. Craft digital trade norms in a more transparent and participatory manner. Of course, the bargaining over national concessions and schedules of commitments must be carried out in the traditional manner so that expert negotiators have sufficient leeway to cut deals. Similarly, it may be that the final decision-making process regarding prescriptions and proscriptions must remain a closed affair (although many would disagree with this view). But in the prior stages of agenda setting and initial formulations, there is no clear reason to maintain secrecy. With respect to data localization and CBDF, following this approach has only raised suspicions and weakened the support for internet openness that might otherwise come naturally to most stakeholders. Governments could use global multistakeholder platforms to solicit input and share proposed texts.

5. In parallel, increase the participation of internet users and other relevant stakeholders in national trade consultation processes. Some regions and countries have made progress in this regard. For example, from 10 January to 26 April 2017 the European Commission (EC) organized a public consultation on Building a European Data Economy. A questionnaire was disseminated to solicit stakeholder views on data localization, access to and re-use of non-personal data liability, and the portability of non-personal data, including interoperability and standards issues.³⁸ In addition, a series of workshops and webinars was held to

further explore the issues. The results of this consultation fed into the EC's mid-term review of its Digital Single Market strategy and will influence its posture on CBDF and related trade issues. Similarly, in May-June 2017, the US government solicited written public comments and potential congressional testimony on proposed revisions to the North American Free Trade Agreement, in which electronic commerce generally and CBDF and data localization specifically are likely to figure prominently.⁹⁹ It would be very helpful if governments which do not do so currently were to organize national consultative processes on data localization, CBDF and related issues.

6. Explore the possibility of establishing a plurilateral agreement on digital trade that includes provisions on data localization and CBDF. Initial participants could include, for instance, members of the OECD and CPTPP signatories, and other countries could join subsequently if and when they are ready. Of course, any such agreement would need to be consistent with the WTO agreements and preferential agreements that have been concluded or are under way. In general, however, it would be ideal to disentangle trade bargaining over internet-related issues from the larger issue sets and controversies at stake in FTAs. In particular, if the free flow of data is conflated in the public mind with controversial proposals concerning investment protections, competition in public services and so on, public support for securing internet openness via trade measures will be difficult to attain.

The World Economic Forum community has considered this option before. For example, participants in the E15 Initiative listed negotiation of a freestanding digital trade agreement as one of their three overarching recommendations. Similarly, the Forum's *Inclusive Growth and Development Report 2017* endorses the idea. Of course, there may be serious arguments for and against splitting digital trade out from larger potential agreements, as well as doing so on a plurilateral rather than multilateral basis. This is an important point for discussion.

Conclusion

The World Economic Forum has shared earlier versions of these recommendations and solicited feedback and input from a diverse group of stakeholders. The Forum has also convened several multistakeholder conversations in 2016-2017 to help an interested community identify a path forward. Those conversations have been bounded by the framework that any efforts must add value to what is already occurring and should be geared towards generating a measurable impact in the near term— recognizing the pace of technological change.

Based on feedback and support, and building on an ongoing programme of work, the Forum will launch a public-private cooperation process drawing from several of the options laid out in this paper. This effort will engage a community of diverse stakeholders to create a process that generates solutions to the root causes of restrictions to data flows and data localization requirements.

Acknowledgements

For their helpful input on the project and feedback on the respective workshop discussion papers, we thank the participants in the workshops held at the World Economic Forum in Geneva on 14-15 September 2016, in San Francisco on 22-23 March 2017, and in Geneva on 25 September 2017.

The World Economic Forum thanks lead author, William J. Drake, International Fellow and Lecturer in the Institute of Mass Communication and Media Research, University of Zurich.

The paper also builds on the analysis presented in, William J. Drake, Vinton G. Cerf and Wolfgang Kleinwächter, Internet Fragmentation: An Overview. The World Economic Forum. January 2016.

http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf

Endnotes

1. James Manyika, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jauch, and Sree Ramaswamy, *Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy*. McKinsey Global Institute, April 2014, p1 <http://www.mckinsey.com/business-functions/strategy-and-corporate-finance/our-insights/global-flows-in-a-digital-age>.
2. For an assessment of the synergistic and cumulative effects of breakthrough advances in digital, physical and biological technologies, see, Klaus Schwab, *The Fourth Industrial Revolution*. The World Economic Forum, 2016 <https://www.weforum.org/about/the-fourth-industrial-revolution-by-klaus-schwab>.
3. For a discussion, see, eBay, *Commerce 3.0 for Development: The Promise of Global Empowerment*. October 2013 <https://www.ebaymainstreet.com/news-events/commerce-30-development-promise-global-empowerment-network>.
4. Independent Experts Advisory Group on a Data Revolution for Sustainable Development, *A World That Counts: Mobilizing the Data Revolution for Sustainable Development*. United Nations, November 2014 <http://www.undatarevolution.org/wp-content/uploads/2014/11/A-World-That-Counts.pdf>
5. US International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*. Publication 4485, Investigation No. 332-540. August 2014, p81 <https://www.usitc.gov/publications/332/pub4485.pdf>.
6. Anupam Chander and Uyen P. Le, "Data Nationalism", *Emory Law Journal*, 64 (2015), pp721-722 <http://law.emory.edu/elj/documents/volumes/64/3/articles/chander-le.pdf>
7. This point is emphasized in, AmCham China, "Protecting Data Flows in the US-China Bilateral Investment Treaty." 2015 <http://www.amchamchina.org/policy-advocacy/policy-spotlight/data-localization>.
8. For an initial effort to estimate the macroeconomic costs, see, Matthias Bauer, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, "The Costs of Data Localisation: Friendly Fire on Economic Recovery", *ECIPE Occasional Paper No. 3.*, European Centre for International Political Economy (2014) http://www.ecipe.org/app/uploads/2014/12/OCC32014_1.pdf
9. Daniel Castro, "The False Promise of Data Nationalism", *The Information Technology & Innovation Foundation*, (December 2013), p1 <http://www2.itif.org/2013-false-promise-data-nationalism.pdf>
10. See, for example, US International Trade Commission, *Global Digital Trade 1: Market Opportunities and Key Foreign Trade Restrictions*. Publication No. 4716, Investigation No. 332-561, August 2017 https://www.usitc.gov/publications/332/pub4716_0.pdf; Internet Association, *National Trade Estimate Report Comments on Digital Trade Barriers*. 2017 <https://cdn1.internetassociation.org/wp-content/uploads/2013/04/InternetAssociation-NTE2017.pdf>; and Google, "Enabling Trade in the Era of Information Technologies: Breaking Down Barriers to the Free Flow of Information." *Transnational Dispute Management*, 1, 2011 <https://www.transnational-dispute-management.com/article.asp?key=1658>
11. Freedom House, *Freedom on the Net 2017: Manipulating Social Media to Undermine Democracy*. November 2017, pp5 & 7 https://freedomhouse.org/sites/default/files/FOTN_2017_Final.pdf
12. Daniel Crosby, "Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments," *E15 Initiative Policy Brief*, E15Initiative (International Centre for Trade and Sustainable Development and The World Economic Forum, March, 2016), p10 <http://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments>
13. Andrew D. Mitchell and Jarrod Hepburn, "Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfer," *Yale Journal of Law and Technology* 19 (2017), pp182-237 http://yjolt.org/sites/default/files/Mitchell_19YJoLT182_0.pdf
14. <http://e15initiative.org/publications/data-moving-across-borders-the-future-of-digital-trade-policy/>
15. Communication from the African Group, "Work Programme on Electronic Commerce, Report of Panel Discussion on 'Digital Industrial Policy and Development'", JOB/GC/133, 21 July 2017, WTO General Council, pp1-2
16. The African Group, "The Work Programme on Electronic Commerce: Statement by the African Group." JOB/GC/144, WTO General Council, 20 October 2017, p2 https://docs.wto.org/Dol2FE/Pages/FE_Search/ExportFile.aspx?id=239609&filename=r/Jobs/GC/144.pdf
17. United States of America, "Measures Adopted and Under Development by China Related to its Cybersecurity Law." Council for Trade in Services, World Trade Organization. S/C/W/374, 26 September 2017, p2 <https://docs.wto.org/dol2fe/Pages/SS/directdoc.aspx?filename=q:/S/C/W374.pdf>
18. WTO, "Report on the Meeting Held 6 October 2017: Note by the Secretariat." S/C/M/133, Council for Trade for Services, World Trade Organization. 6 November 2017, p19

19. Trans-Pacific Partnership, "Chapter 14: Electronic Commerce," 2015, pp14-5 & 14-7 <https://www.mfat.govt.nz/assets/securedfiles/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf>
20. Brussels Declaration on Trade and the Internet (15 March 2016). https://www.eff.org/files/2016/03/15/brussels_declaration.pdf
21. i2Coalition, "We Support The Goals Of The Brussels Declaration On Trade" (22 February 2016). <https://www.i2coalition.com/support-goals-brussels-declaration-trade>
22. Global Commission on Internet Governance, Our Internet (Centre for International Governance Innovation and Chatham House, 2016), p78 <https://www.ourinternet.org/report>
23. NETmundial Multistakeholder Statement, 24 April 2014, pp4-7. <http://netmundial.br/wp-content/uploads/2014/04/NETmundial-Multistakeholder-Document.pdf>
24. Dillon Reisman, "Where Is Your Data, Really?: The Technical Case Against Data Localization", Lawfare 22 May 2017, <https://www.lawfareblog.com/where-your-data-really-technical-case-against-data-localization>
25. See, for example, Jennifer Daskal, "The Un-Territoriality of Data", Yale Law Journal, Vol. 125, November 2015, pp326-398 <http://www.yalelawjournal.org/article/the-un-territoriality-of-data>; Andrew Keane Woods, "Against Data Exceptionalism", Stanford Law Review, Vol. 68, April 2016, pp729-789, <https://www.stanfordlawreview.org/print/article/against-data-exceptionalism>; and Dan Svantesson, "Against 'Against Data Exceptionalism'", Masaryk University Journal of Law and Technology, Vol. 10:2, 2016, pp200-211. <https://journals.muni.cz/mujlt/article/view/5925/6029>
26. On the growing role of networks in the governance mix, see, Slaughter, Anne-Marie, *The Chessboard and the Web: Strategies of Connection in a Networked World*, Yale University Press, 2017
27. For a discussion, see, Joost Pauwelyn, "Rule-Based Trade 2.0? The Rise of Informal Rules and International Standards and How they May Outcompete WTO Treaties", *Journal of International Economic Law*, Vol. 17, 2014, pp739-751 http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474525
28. As per, Amadine Orsini, Jean-Frédéric Morin, and Oran Young, *Regime Complexes: A Buzz, a Boom, or a Boost for Global Governance?*, *Global Governance* Vol.19, 2013, pp27-39
29. G7, "Joint Declaration by G7 ICT Ministers", May 2016, p3 http://www.japan.go.jp/g7_userdata/common/data/000416959.pdf
30. "G20 Digital Economy Development and Cooperation Initiative", September 2016, p3, <http://www.g20.org/English/Documents/Current/201609/P020160908736971932404.pdf>
31. B20, *Digitalization for All: Future-Oriented Policies for a Globally Connected World*, 2017, p16, https://www.b20germany.org/fileadmin/user_upload/documents/B20/B20_Digitalization_Policy_Paper_2017.pdf
32. For illustrations of the dynamics of such orchestration, see, Kenneth W. Abbott and Duncan Snidal, "Strengthening International Regulation Through Transnational New Governance", *Vanderbilt Journal of Transnational Law* 42, 2009, pp501-78
33. United Nations Conference on Trade and Development, *Data Protection Regulations and International Data Flows: Implications for Trade and Development*, UNCTAD, 2016, p56, http://unctad.org/en/PublicationsLibrary/dtlstict2016d1_en.pdf
34. Organization for Economic Cooperation and Development, *Key Issues for Digital Transformation in the G20: Report Prepared for a Joint G20 German Presidency/OECD Conference, Berlin, 12 January 2017*, p157, <https://www.oecd.org/g20/key-issues-for-digital-transformation-in-the-g20.pdf>
35. European Services Forum, "Cross Border Data Flows: An Imperative for All Trading Companies in a Global World – ESF Position Paper," 10 May 2013, p4, <http://www.esf.be/new/wp-content/uploads/2015/01/ESF-Position-on-Cross-border-data-flows-10-May-2013-Final.pdf> (emphasis added)
36. Joshua P. Meltzer, "Maximizing the Opportunities of the Internet for International Trade," E15 Expert Group on the Digital Economy – Policy Options Paper, International Centre for Trade and Sustainable Development and The World Economic Forum, 2016, p22, <http://e15initiative.org/publications/maximizing-opportunities-internet-intrnational-trade>
37. The materials associated with the EC's public consultation on the European Data Economy, <https://ec.europa.eu/digital-single-market/en/news/public-consultation-building-european-data-economy>
38. The US government's request for comments is per usual posted in the Federal Register, <https://www.gpo.gov/fdsys/pkg/FR-2017-05-23/pdf/2017-10603.pdf>. Comments filed and related materials are at <https://www.regulations.gov>



COMMITTED TO
IMPROVING THE STATE
OF THE WORLD

The World Economic Forum, committed to improving the state of the world, is the International Organization for Public-Private Cooperation.

The Forum engages the foremost political, business and other leaders of society to shape global, regional and industry agendas.

World Economic Forum
91–93 route de la Capite
CH-1223 Cologny/Geneva
Switzerland

Tel.: +41 (0) 22 869 1212
Fax: +41 (0) 22 786 2744

contact@weforum.org
www.weforum.org