WORLD ECONOMIC FORUM

COMMITTED TO IMPROVING THE STATE OF THE WORLD

BACKGROUND PAPER

for the workshop on
Data Localization and Barriers to Transborder Data Flows
14-15 September 2016
The World Economic Forum
Geneva

William J. Drake
The University of Zurich
william.drake@uzh.ch

The views expressed in this paper are those of the author and do not necessarily represent the views of the World Economic Forum or its Members and Partners

CONTENTS

Introduction

This background paper was prepared for the workshop on *Data Localization and Barriers to Transborder Data Flows* held at The World Economic Forum in Geneva on 14-15 September 2016. The workshop is a joint effort of the Forum's System Initiatives on the Future of Digital Economy and Society and the Future of International Trade and Investment. It seeks to build upon the report *Internet Fragmentation: An Overview* and the E15 Initiative reports released at the Forum's Annual Meeting in Davos earlier this year (in particular *Maximizing the Opportunities of the Internet for International Trade*)[1] by creating a structured process of multistakeholder dialogue and analysis to map and assess:

- The various concerns expressed by governments and certain stakeholders with respect to transborder data flows generally and specific categories thereof
- Governmental actions that have been or could be taken in response to these concerns
- Current and potential impacts of such actions, both positive and negative, from the standpoints of economic growth and innovation, political-legal issues, socio-cultural issues, etc.
- The least restrictive/discriminatory approaches to addressing some of the most salient of these issues and concerns in order to provide a more informed basis for policymaking by governments and their dialogues with stakeholders.

This paper is not a report of research findings. Rather, it is merely intended to facilitate conversation at the workshop by helping to tee up the issues to be addressed. Accordingly, at the end of each section the paper offers a few possible discussion points that participants might wish to take up alongside any other items they care to identify.

The starting point for this initiative is the reality that, as Lee Tuthill observes, "The increasing tendency to regulate cross border data flows is a universal phenomenon common to both developed and developing economies."[2] But the foundational challenge we face is the dearth of systematic information about the incidence of such regulations, e.g. exactly which categories of data used by which firms and industries are being subjected to localization requirements or barriers to transborder data flows (TDF) by which governments using which measures. We appear to lack mechanisms to systematically track and monitor such practices across sectors and countries, so much of the debate is based on variable aggregations of anecdotal evidence or extrapolations from a core set of particularly noteworthy examples. Considering the options for improvement of our collective knowledge base is therefore an important task.

The stakes here are high. Data flow has become the lifeblood of the global information economy, and the Internet and other electronic networks are its circulatory system. As McKinsey estimates, total cross-border Internet traffic increased 18-fold from 2005 to 2012,[3] and "data flows account for US$2.8 trillion of global GDP in 2014 and "cross-border data flows now generate more economic value than traditional flows of traded goods."[4] In a related vein, Robert Pepper and colleagues observe that:

> 61 percent (US $383.7 billion) of total US service exports were digitally delivered in 2012, and 53 percent of total US imports were digitally delivered. In absolute terms, the amount of digitally delivered exports and imports is even larger in the European Union, which digitally delivered US $465 billion in exports in 2012 and spent US $297 billion on imports. Digital trade is credited with an estimated increase in US gross

> domestic product (GDP) of 3.4 percent to 4.8 percent in 2011 and with the creation of up to 2.4 million jobs…[5]

The new business models and markets that will increasingly drive the fourth industrial revolution[6] 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. TDF will be foundational to what Cisco calls "the Internet of Everything (IoE)"--- the confluence of people, process, data, and things---in which "between 2013 and 2022, $14.4 trillion of value (net profit) will be "up for grabs" for enterprises globally."[7] But the unchecked accumulation of blockages to data flow could greatly diminish the prospects for this evolution and all that it could entail in terms of socio-economic development and personal empowerment.

We need to get an analytical and empirical handle on the twin problems of data localization and barriers---not only their scope and impact, but also their root causes and the design of governance mechanisms that could help mitigate their negative effects. International trade policy instruments likely will play important roles in the search for solutions, so the meeting will need to consider the relevance of the World Trade Organization's (WTO) General Agreement on Trade in Services (GATS), the Trans-Pacific Partnership (TPP), the Transatlantic Trade and Investment Partnership (TTIP), and the Trade in Services Agreement (TiSA), among others. However, the prospects for progress on digital trade in these frameworks are unclear at best given the wider politics of trade at the national and international levels.

Moreover, in the case of Internet-related issues there are additional complications. Not only is there an especially keen level of interest and indeed mistrust in international trade agreements among many denizens of the 24/7 globalized infosphere who fear that secret deals will be made that could curtail their freedom to create, access, and disseminate information. But such sentiments are by no means limited to the sort of anti-globalization civil society activists that are familiar to trade policy makers. They are also evident to varying degrees among the wide array of people and organizations active in the multistakeholder Internet governance community, e.g. in spaces like the Internet Governance Forum (IGF), the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), the Regional Internet registries (RIRs), the Internet Society, and so on. 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 acclimated 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.

A priori, trade policymakers might expect that a shared commitment to an open and unfettered Internet would translate into full-throated support from the Internet community for tackling barriers to data flow through the abovementioned agreements. But it may not. There is reasonably widespread skepticism and reluctance to embrace decisions about the Internet that are reached in a closed intergovernmental rather than open multistakeholder fashion, and which can be perceived as favoring the special interests of powerful governments and companies at the expense of the global public interest. The widespread perceptions of the TPP, which after all entails some quite progressive provisions with respect to data flow and electronic commerce, illustrates the dilemma. Building understanding of and support for the positive role trade instruments can play alongside other more participatory initiatives may require a new form of engagement and some hybrid, two-track diplomacy. These process issue also merit consideration in the workshop.

This paper is organized as follows. Section 1 provides some historical background on the growth of perceived tensions between national sovereignty and TDF, as these may well have echoes in the current policy environment. Section 2 highlights the contemporary challenges of data localization policies and barriers to TDF. Section 3 turns from the problems to potential solutions by putting on the table the role of international trade policy instruments and other potential governance frameworks. Finally, the Conclusion briefly looks forward to the possible shape of this WEF initiative in the coming months.

1. Historical Background: National Sovereignty and Transborder Data Flows

Current discussions of these issues sometimes give the impression that they first arose quite recently, in particular with the growth of cloud computing and the Snowden revelations. But of course, the question of data localization and flow have been with us for at least 40 years and antedate the global public Internet, and the broader question of how to govern the cross-border flow of information goes even further back to the mid-19th century. As such, framing the issues narrowly as just a sudden rise of digital protectionism akin to what ails the agricultural, manufacturing and services sectors generally can obscure the thinking and multidimensional issues at play. Hence it is useful to step back and place the issues in a broader historical context.

The jealous protection of national sovereignty has been foundational to international communications and information policy since the dawn of international telegraphy. As with international postal agreements, in the bilateral and multilateral treaties of the 1840s-1860s, governments were careful to codify mutually exclusive control of their respective national networks and to limit international regimes to just the connections between these. Moreover, the 1850 Treaty of Dresden that created the Austro-German Telegraph Union held that “the telegraph offices...are required to refuse to accept or transmit those private messages whose content offends against the laws or which are deemed to be unsuitable for communication on grounds of public good or morality.”[8] The 1865 Treaty of Paris establishing the International Telegraph Union elaborated on this in provisions that have been foundational to international communications law ever since. As the 2014 Constitution of the International Telecommunication Union (ITU) specifies,

> 180. Member States reserve the right to stop, in accordance with their national law, the transmission of any private telegram which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency, provided that they immediately notify the office of origin of the stoppage of any such telegram or any part thereof, except when such notification may appear dangerous to the security of the State.
>
> 181. Member States also reserve the right to cut off, in accordance with their national law, any other private telecommunications which may appear dangerous to the security of the State or contrary to its laws, to public order or to decency.[9]

In short, national sovereignty is understood by many as not simply a constitutional principle under which states are jurisdictionally separate and equal, enjoy the same rights and privileges, and are not bound by a higher supranational authority in the anarchical international political system. This legal and horizontal principle is complemented by an operational and vertical premise: national polities are hierarchically organized, and states can configure and govern their national networks and usage however they please as long as they play by the rules where international correspondence is concerned. Sovereignty has in the thinking of many become equated with inviolable independence of action, and the lengths to which governments have gone to maintain this of course have varied and continue to do so today in accordance with various historical and political conditions. Moreover, in the years to follow the onset of collaboration in telecommunications, the paramount importance of sovereignty was successively reiterated in a slew of subsequent international institutions pertaining to e.g. radio frequencies, satellite orbital slots, satellite systems, broadcasting and information flow, security and more.[10]

It was against this backdrop that the matter of corporate TDF first arose in the mid-1970s. Recall the tenor of the times: much of the post-colonial world was embarking on various degrees of socialist economic organization; the Non-Aligned Movement and the Group of 77 were thriving; the “global South” was pushing, particularly in the UN Conference on Trade and Development (UNCTAD), for a “New International Economic Order” it hoped would effectively transfer wealth, technology and trade advantages from the global North; a parallel campaign was getting underway, particularly in the United Nations Educational, Cultural and Social Organization (UNESCO) for a “New World Information and Communication Order” that would *inter alia* require the licensing of journalists, enhanced abilities for governments to keep out unwanted transmissions of news and other information, and a “balanced” flow of information between the global North and South; and there were heated new global debates underway about both the influence of transnational corporations and the comparative technological prowess of the United States in the emerging information age. It was in this context that the Organization for Economic Cooperation and Development (OECD) first took up the transmission of data over corporate networks and across national frontiers.

At a 1974 conference, an OECD expert group coined the term "Transborder Data Flow (TDF)," and raised the question of whether it "constituted a problem sufficiently important in its implications for national sovereignty for governments to propose regulatory action."[11] The OECD then set up a Working Party on Transborder Data Flows and spent the next decade delving into the perceived potential effects of corporate TDF on nation-states’ economic, legal, social, and political independence, all which were frequently framed in terms of challenges to national sovereignty.

Active in parallel was the Intergovernmental Bureau of Informatics (IBI), based in Rome. The IBI comprised governments from Latin American (13), Africa (18), the Middle East and North Africa (6), as well as Spain, Italy and France, which covered much of its costs. Participation in its various international meetings on TDF, including World Conferences held in 1980 and 1984, was substantially broader than these 40 members, and a frequent organizing assumption of its deliberations was that TDF was an issue that required a new global regulatory regime. Delegates from 78 governments attending a 1978 IBI conference endorsed a report warning that TDF could place national sovereignty in jeopardy.

Similarly, in 1979, a committee of the Canadian government suggested that TDF "poses possibly the most dangerous threat to Canadian sovereignty.” A report by the Commission of the European Community (EC) worried that foreign control of TDF and related industries threatened "a reduction in [Europe's] independence in decision-making in all walks of public and private life." In 1982, the President of France said that the use of TDF for the "dissemination of information processed and largely controlled by a small number of dominant countries could cause the rest to lose their sovereignty."[12] And so on…these were by no means isolated statements.

For narrative purposes, one could say that the TDF issue has evolved through three semi-distinct stages. From 1974-1981, during what we could call TDF 1.0, the dominant focus was on data protection and personal privacy. Then as now, the key axis of tension was trans-Atlantic, with European governments favouring omnibus laws and the establishment of data protection bodies while the US pursued a piecemeal and more permissive approach. Canada was an important bridge between these two positions. Years of work in the OECD resulted in the adoption in 1980 of voluntary Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, an important and anodyne set of recommendations establishing principles regarding e.g. collection limitation, data quality, purpose specificity, use limitations and the like. These were revised for the Internet age in 2013.[13] The USA launched a campaign to get its companies to endorse the guidelines, but this did not entirely put the issue to rest.[14] In the next year, the Council of Europe adopted its Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, an instrument with nominally a bit more bite. In the years to follow the main action shifted to the European Union, which proceeded to establish its own mechanisms beginning with the 1995 Data Protection Directive.

As the privacy debate unfolded, participants began to raise a wide range of economic, legal, and social concerns they believe could be negatively impacted by corporate data flows. The period of 1981-1985, which could be called TDF 2.0, was consumed with assessing these non-personal data issues. Attention focused on both intra-corporate and inter-corporate transfers (the former was thought to comprise about 90% of traffic) whether conducted via proprietary data protocols like IBM's Systems Network Architecture, closed user group networks such as the Society for Worldwide Interbank Financial Telecommunications, value-added networks such as TYMNET, TELENET, and Satellite Business Systems, or by consortia of Ministries of Posts, Telegraphs and Telephones (PTTs) such as EURONET and DIANE. The debate played out not only in the OECD and the IBI but also in a rapidly expanding global community of expertise and practice that had its own journals, conferences, and the like, and was a boon to consulting houses whose clients were worried by the prospect of new regulations.

Already during the privacy debate Brazil had adopted rules requiring the prior approval of data transmission links, the maintenance in country of duplicate copies of certain data bases, and the local data processing of data unless a company's needs could not be met thereby.[15] Multinational companies feared that this approach would spread. Moreover, there were growing calls, particularly by the French government in the OECD and by a number of countries in the IBI, for a new international regulatory regime. At the IBI's Second World Conference on TDF in 1984, the working document proposed as regime principles the "Recognition of rights inherent to the sovereignty of States which forsee that [TDF] serve their interests and objectives," and that "TDF shall not violate their sovereignty nor their constitutional and legal principles."[16]

Some of the non-privacy concerns raised in the course of the debate included:

a. Legal Issues

- *"Information sovereignty:"* some governments saw information from or about their countries as a natural resource over which they should have exclusive legal authority. Data gathered by remote sensing satellites was often cited as an example.
- *Access to data held abroad: there were* fears that data about national persons, assets, or events would be held in remote "data havens" from which it could not be retrieved when needed.

- *Vulnerability interdependence:* reliance on transnational systems in which data is remotely located and could break down and leave countries unable to perform crucial functions. This became a particular cause of concern to Sweden.
- *Liability:* errors in transmissions in transnational networks raised questions of pinpointing the source of problems and assigning responsibility for damages.
- *Extraterritorial application of national laws:* foreign governments could assert authority over data held within a country's territory, or apply export controls limiting the transfer of information to third parties like the Soviet Union.
- *Intellectual property protection:* it could be difficult to ensure disparate national laws were applicable and enforceable, or conversely to avoid being subject to claims based on another jurisdiction's laws.
- *Computer-related crime:* actions taken abroad could impact locally without any means of remediation.
- *Regulation of corporate behavior:* TDF could allow firms to circumvent government policies concerning taxes, rule compliance capital restrictions, etc.

b. Economic Issues

- *Location of corporate decision-making:* firms could centralize decision-making activity in their home countries at the expense of host countries.
- *Location of production and other non-managerial functions:* the global reallocation of activities to reduce costs could impact local employment, job quality, etc., perhaps with less sophisticated and skilled operations being relegated to the host countries.
- *Network-based trade in services:* high-tech enabled foreign firms could be virtually present within host markets and create new forms of competition in which local companies are disadvantaged.
- *Financial regulation and competition:* particular attention was devoted to the challenges of 'hot money' being moved instantaneously in ways that could challenge the efficacy of domestic policies and institutions.
- *New networked organizational structures:* the deepening of relationships between technologically capacitated firms could give rise to alliances and other formations that were more difficult to monitor or regulate using existing policy tools.
- *Commodification of information*: TDF appeared to be bound up with a wider trend toward information becoming a proprietary strategic asset to which access was uneven, including information drawn from public sources.
- *Valuation and taxation:* France in particular felt that lucrative TDF transactions should be taxable like any product, but it was difficult to assess how this could be done.

c. Socio-Cultural Issues

- *Cultural construction and effects on national identity:* the notion that data's formulation carriers with it certain values and ideas that inform its organization and may be alien to local cultures.
- *The global spread of English:* as the "official" language of business and professions.
- *The information rich and the information poor:* divisions between those who have access to and can use data vs. those who are left out but may be impacted by decisions.
- *Stifling the development of indigenous on-line cultural products:* the head-start of foreign companies, especially from the USA, could preclude the development of locally owned and appropriate products.

As the above list indicates, the growing importance of data and its flow to multinational firms was viewed as a multidimensional set of challenges that in the aggregate appeared to some governments to weaken their sovereign abilities to enforce national policies and compete in what was then a landscape of very unevenly distributed capabilities. Unsurprisingly then, there was a fairly notable degree of advocacy for new regulations that would somehow protect countries from these potential problems. But the problem for proponents of regulations was a lack of hard, systematic evidence that the anticipated negative effects were transpiring and directly due to TDF. The same relatively small set of anecdotal examples of problems was trotted out and redeployed repeatedly to support a wide range of claims, and governments lacked the ability to peer within corporate networks in search of "aha!" moments.

In the end, a sustained campaign by global business and key governments like the United States successfully took off the table much of what had been thrown on it. As the momentum for new interventionist measures evaporated, France and Brazil quit the IBI, and the financially struggling organization was forced to shut down. Much of the OECD's work was narrowed and redirected toward advancing the then new international trade in services agenda, with responsibility shifting from the Working Party on TDF to the OECD's Trade Committee. And to draw a line under the matter, in 1985 the OECD Adopted its Declaration on Transborder Data Flows, a document that was a far cry from what the pro-regulatory forces had once imagined. Among other things, member governments declared their intention to:

> 1. Promote access to data and information and related services, and avoid the creation of unjustified barriers to the international exchange of data and information;
> 2. Seek transparency in regulations and policies relating to information, computer and communications services affecting transborder data flows;
> 3. Develop common approaches for dealing with issues related to transborder data flows and, when appropriate, develop harmonized solutions;
> 4. Consider possible implications for other countries when dealing with issues related to transborder data flows.[17]

In the years to follow, the meaning of the term TDF seems to have collapsed back to where it started, that is, as pertaining first and foremost to the transnational movement of personally identifiable information and the attendant questions of data protection and privacy. The most robust continuing discussion of "TDF" today take place among data protection commissioners and related stakeholders, and in the pages of journals like *International Data Privacy Law.* In other contexts the term seems to have fallen out of favor and been replaced by other phrases that arguably are no better, like "cross-border data flows" (CBDF?) or "transnational data flows." And some of the non-personal data issues that had been raised have been recycled into broader debates about today's global Internet (and discussed as if entirely new), or have in some cases resurfaced in discussions of global trade in services.

While the intellectual and political landscape has changed dramatically since the days of TDF 1.0 and 2.0, some of the core dynamics that animated those debates arguably are still with us in what could be called today's TDF 3.0. Three in particular may merit consideration.

1. Some governments continue to equate national sovereignty with a very high degree of independence that they believe could be challenged by unregulated TDF. This seems to be most clearly evidenced by aspects of China's push for "cyber-sovereignty," Russia's approach to its "national Internet segment," the recently announced "Iranian Internet" and similar cases, but a keen concern to avoid the

perceived diminishment of control is likely to be common across political systems. How can misguided concerns be effectively allayed when the sovereignty framing is invoked? Is a trade discourse sufficient in this context?

2. Some of the specific issues that were raised in the previous debates remain unresolved and politically salient vis. today's global Internet. Data protection and privacy as well as access to information held abroad present obvious examples, but others that one might regard as less persuasive or even real may leave some imprint on contemporary thinking as well. Which of these issues, if any, seem currently or potentially relevant to data localization and TDF barriers? If we could somehow "solve" privacy and access (in the latter case via improved MLATs etc.), could any remaining issues be dealt with entirely through trade processes?

3. It is common in global governance discussions to hear it said that we need to take a holistic approach to issue-areas. But one consequence of doing so can be that, as in earlier TDF debates, issues of varying tractability are continuously put on the table until it becomes piled high and difficult to manage. Is there a risk that calling attention to localization and barriers as a defined issue-area could take us down a similar path? Could a more piecemeal approach be preferable?

2. Data Localization and Barriers to Transnational Data Flows

As the thumbnail history above indicates, data localization and barriers are not new phenomena. In fact, in some particularly sensitive sectors they may be more the norm than exceptions to the rule. For example, one suspects that many governments apply such restrictions to certain types of public sector information, especially with respect to national security and law enforcement matters. The same may true of some aspects of financial services, which might complicate US efforts to "fix" the carve-out in the TTIP. Again, it would be very useful to obtain systematic empirical data on the prevalence of such requirements in these and other sectors, but we do not have the mechanisms in place.

By default then, surveys provide the best aggregate indicators of the scope of the problems. As yet there are not an abundance of these, but what we do have presents some fairly provocative evidence. With regard to localization, the US International Trade Commission reported in 2014:

> Firms perceive localization barriers to international digital trade differently, depending on sector and firm size. Eighty-two percent of large firms and 52 percent of SMEs in the digital communications sector felt that localization requirements presented obstacles…The highest percentages of large firms that felt that localization barriers were 'substantial or very substantial' obstacles were in digital communication (34 percent) and content (27 percent), th
> percent of large firms in the finance sector also believed them to be 'substantial or very substantial' obstacles. Of SMEs, 21 percent of firms in finance, 16 percent of firms in the other services sector, and 15 percent of digital communications firms believed localization requirements to be "substantial or very substantial" obstacles.[18]

Of course, this does not tell us exactly what kinds of obstacles are being encountered and where. That said, the available evidence suggests that data localization requirements may take the following forms:

1. Data must be processed by entities physically within a national jurisdiction.
2. Data processing may require a specific level of "local content," or the use of locally provided services or locally manufactured equipment.
3. Data must be locally stored or "resident" (as distinct from "data retention" policies imposed on Internet service providers for law enforcement purposes).
4. Data processing and/or storage must conform to national rather than internationally accepted technical and operational standards.
5. Data must be routed largely or solely within a national or regional space when possible.
6. Data may not be transferred out of the national jurisdiction via networks.[19]

With regard to the fifth possibility, there are not a lot of obvious examples of it being pursued. The much-discussed "Schengen area" routing scheme has not come to pass. North Korea and Cuba may provide qualitatively different examples, whether partially or in full. Moreover, except where data is actually prohibited from leaving such an area, it is not clear just how damaging such routing requirements would be to the overall Internet (engineers I have discussed this with seem divided). Given the size and importance of the country, it will be interesting to see what exactly the recently announced "Iranian Internet" will mean in practice; the government's announcement suggests that it will be "increasing the share of internal traffic for consumers," but this may just refer to the use of IXPs.[20]

With regard to barriers to TDF, there is perhaps an even bigger problem in acquiring systematic evidence. If a government announces a standing localization policy one may be able to acquire clear information about what is involved, but barriers to data flows often can be more ephemeral and negotiable. Moreover, there is a significant difference between actually prohibiting data flow or requiring prior consent, on the one hand, and actions that may simply make data flows less attractive, on the other. Sometimes what gets reported as a barrier may simply involve financial or operational disincentives and friction, rather than an actual prohibition. Consider, for example, this figure from the Business Roundtable's study:

Figure 1

Local Data Storage	Restricts data flows by requiring specified data — often but not always personal information — to be stored on local servers. May also require specific applications or services to operate in-country, processing data locally to avoid offshore transfer.
Data Protection	Restricts data flows through application of data privacy laws with adequacy and/or consent requirements that cannot reasonably be met without local data storage.
Geolocation Data Privacy	Restricts data flows by preventing the collection, disclosure, transfer or storage of geolocation data without an individual's consent.
Local Goods, Services or Content	Restricts data flows by requiring use of locally provided services or locally generated content. May also require use of domestically made or locally sourced equipment — limiting choice and perhaps efficiency but not data flows per se.
Government Procurement	Restricts data flows by limiting government procurement of foreign goods or services — for example, restricting information technology and communications contracts to locally delivered services.

Online Censorship	Restricts data flows by blocking or filtering information transferred into or out of a country.
Government Investment/Tax	Affects data flows by using tax incentives to promote use of local content (defined above) or labor.
Ownership/ Employment	Affects data flows by requiring in-country subsidiaries, branch offices or representation. May influence data flows by limiting foreign ownership or requiring joint ventures.
Local Production	Affects data flows by requiring local production of goods or services as a condition of market access — for example, requiring local data centers to deliver in-country services.
Payment Card Regulations	Affects payment data flows by requiring payment information to be stored locally.
Export Control	Affects data flows by requiring corporate intellectual property and other technology to reside in-country.
Forced Transfer of Intellectual Property	Affects data flows by requiring companies to transfer intellectual property to the countries in which they do business.
Traffic Routing	Affects data flows by requiring communications providers to route Internet traffic in a specific way.

Source: Business Roundtable, 2015. *Putting Data to Work: Maximizing the Value of Information in an Interconnected World,* The Business Roundtable, p.18.[21]

Undoubtedly, the policies listed in the left hand column can raise the costs of doing business and make transferring data across borders unattractive or at times impossible. Nevertheless, there are notable differences between some of the examples listed. For example, government tax incentives promoting local content or labor do not necessarily prohibit TDF in the same outright manner as censorship. Similarly, there may be a requirement to preserve copies of certain data on local servers without actually prohibiting such data from moving out of the country. In short, we need to be as precise as possible about what we mean by barriers to TDF and its growth around the world. If the issue involved is actual blockages that is one thing, but if it is more a matter of uncertainties, operational difficulties, and increased costs that is something else---not only analytically, but politically when dealing with the governments involved. What is needed is a clear typology of barriers that clearly characterizes the precise modalities involved in different classes of cases.

The examples above also point to another and more controversial matter concerning what “counts” as data localization and barriers that the group may wish to address. This concerns the fraught issue of data protection and personal privacy. It is not unheard of for some industry advocates to characterize the sort of measures taken in Europe as being roughly akin to other policies that may be pursued for very different purposes, like simple economic protectionism or political control. And it is also not unheard of for people to suggest that all such policies constitute trade barriers and should be subject to trade disciplines.

In contrast, advocates of privacy protection generally insist that such measures should viewed as an entirely separate matter that stems from human rights laws and the social contract rather than any techno-nationalist or protectionist instincts, and that as such the issues must not be dealt with through trade rules. Moreover, they argue that privacy protection is qualitatively different from “forced localization” and barriers since the issue would disappear if e.g. the United States chose to implement stronger privacy laws. This argument has been with us since the early days of the TDF debate in the 1970s and seems likely to persist irrespective of the recent Privacy Shield agreement.

Adding to the complexity is the fact that strict privacy rules requiring local processing and/or retention and prohibitions on flows of personally identifiable information have been introduced by some governments that are not otherwise known to be keen protectors of privacy and other civil liberties. While this would obviously present challenges, it may be that a differentiated approach to the topic would be justified.

However one views this matter, there seems to be a growing consensus among close observers that localization and barriers pertaining to non-personal data do not achieve their nominal objectives, and that they imposes restrictions that are greater than what is required to achieve any legitimate national goals. It also stands to reason that broad-scoped policies may be more damaging than finely targeted ones.

For example, 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 centers and the few companies servicing these centers locally.”[22] In addition, preliminary evidence suggests that localization policies can have a notable negative effect on GDP.[23]

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 foreign 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.”[24] It may also be that multinational companies are more likely to effectively guard their customers’ data than some of the local alternatives. And of course, barriers to the movement of data and information across borders in themselves can be viewed as inconsistent with international human rights obligations.

While intergovernmental discussions proceed in trade and other forums, progress on this nexus of issues might also be pursed from a multistakeholder angle. If their proponents believe that localization and barriers are simply things that are disliked by “big companies that can afford it” or inconsistent with other governments’ preferences, they may not feel compelled to reconsider the issues. Perhaps they need to hear from the companies effected, particularly small and medium-sized enterprises, as to exactly how such policies confound business operations in a manner that is to their countries’ detriment. They also may need to hear from people in the technical community what such actions may mean for the Internet and its evolution within their countries, and from their national business communities (other than any beneficiary suppliers) and civil society as to how the policies may limit their respective abilities to contribute to economic and social development. A dialogue about concrete effects on the ground would lend needed local weight to the arguments of outside analysts and stakeholders.

Three items workshop participants may wish to discuss could include:

1. A WEF initiative could take stock of the cases raised in the publicly available literature and, if the information allows, attempt to devise a taxonomy of the types of measures in place and the scope of their impact (e.g. by firms or types of data). But given the lack of systematic comparative data, other steps may be needed to paint a compelling picture that illustrates the significance of the problem. One option might be some brief anonymized case studies (e.g. presented in boxes) based on interviews with impacted companies and stakeholders. Are there other near-term ways in which the knowledge gaps could be filled?

2. How can the negative effects of localization and TDF barriers best be conveyed to the governments involved? What sort of evidence, strategies, alliances, and so would be needed to press the case effectively?

3. How should we deal with the problematic issue of personally identifiable information? This problem will only become more pervasive as we evolve toward the Internet of (every)things. Can we draw defensible distinctions between privacy measures that are grounded in human rights concerns and privacy measures that are actually employed for protectionist purposes? Should privacy issues be addressed separately from discussions of localization and related trade disciplines? If, as some are already saying, the Privacy Shield is insufficient, how do we proceed?

3. International Trade Agreements and Other Governance Frameworks

The WTO's GATS is very much a product of the pre-Internet era of digital trade. By the time it had entered into force on 1 January 1995 the world economy was on the edge of a sea change, and the Uruguay Round discussions of value-added telecommunications networks, private corporate networks run on leased circuits and proprietary platforms, and computer and information services already seems a bit dated. The years immediately after were preoccupied with negotiating the basic telecommunications agreement, and it was not until 1998 that the WTO launched the Global Electronic Commerce Work Program. The questions taken up---classification, competition and domestic regulation, safeguards, customs duties, nondiscrimination and the problem of "likeness" and so on---were of sufficient complexity and novelty that many trade ministries lacked clear positions and the discussions dragged on endlessly without a notable sense of inspiration.[25] Happily, the 10th Ministerial Conference at Nairobi in December 2015 agreed to reinvigorate the program, and it is said there has been signs of progress since. In this context, in July 2016 the United States released a non-paper that spoke directly to our issues by noting, *inter alia,*

> 2.3. ENABLING CROSS-BORDER DATA FLOWS: Companies and consumers must be able to move data as they see fit. Many countries have enacted rules that put a chokehold on the free flow of information, which stifles competition and disadvantages digital entrepreneurs. Appropriately crafted trade rules can combat such discriminatory barriers by protecting the movement of data, subject to reasonable safeguards like the protection of consumer data when exported. P.2
>
> 2.4. PROMOTING A FREE AND OPEN INTERNET: A free and open Internet enables the creation and growth of new, emerging, and game-changing Internet services that transform the social- networking, information, entertainment, e-

> commerce and other services we have today. The Internet should remain free and open for all legitimate commercial purposes.
>
> 2.5. PREVENTING LOCALIZATION BARRIERS: Companies and digital entrepreneurs relying on cloud computing and delivering Internet-based products and services should not need to build physical infrastructure and expensive data centers in every country they seek to serve. Such localization requirements can add unnecessary costs and burdens on providers and consumers alike. Trade rules can help to promote access to networks and efficient data processing.

But it also acknowledged that, “The United States perceives that WTO Members remain in a period of defining terminology, studying implications, and considering in a deliberate fashion how best to approach new WTO work on e-commerce/digital trade.”[26] So it is not clear how quickly one can expect significant progress in this space.

Nevertheless, there may be grounds for cautious optimism. As Mira Burri notes, “For computer and related services, which was a fairly new sector at the time of the Uruguay Round and thus was largely devoid of domestic regulation, as well as of trade barriers, essentially all WTO Members have made far-reaching commitments for both market access and national treatment. These include key sub-sectors, such as data processing services and data base services, which correspond to many of the essential Internet businesses, such as search engines. Overall, computer and related services marks a very high level of liberalization and the wiggle-room available for domestic regulators is thus severely limited.”[27]

Moreover, the dispute settlement system lent an additional hand to data flows in the US-gambling case. The report concluded that

> ... mode 1 [cross-border supply] under the GATS encompasses all possible means of supplying services from the territory of one WTO Member into the territory of another WTO Member. Therefore, a market access commitment for mode 1 implies the right for other Members’ suppliers to supply a service through all means of delivery, whether by mail, telephone, Internet etc., unless otherwise specified in a Member’s Schedule. We note that this is in line with the principle of ‘technological neutrality’, which seems to be largely shared among WTO Members. Accordingly, where a full market access commitment has been made for mode 1, a prohibition on one, several or all means of delivery included in this mode 1 would be a limitation on market access for the mode.[28]

With this ruling and the reality that many governments have submitted schedules of commitments with “None” marked in the “Limitations on market access” column for computer and information services, there are grounds to believe that the existing framework is suitably attuned to the problems of data localization and flow. Questions of interpretation need to be worked through, but one could argue, as per Daniel Crosby, that “An analysis of existing WTO law leads to the conclusion that data localization measures violate existing GATS rules and commitments to allow unrestricted cross-border trade in digital services and cross-border data flows.”[29] An important order of business then, as the E15 group recommended, is to “Clarify the application of WTO members’ GATS commitments to digital trade.”[30]

Beyond assessing these commitments, further consideration of the implications of the Annex on Telecommunications’ implications for emergent data flow barriers would seem apt. The Annex sets out robust guidelines for access to and use of public telecommunications transport networks and services in sectors where countries have undertaken specific commitments, which benefits suppliers of any scheduled service. In an echo of the prior TDF debates, it includes a provision that "Each Member shall ensure that service suppliers of any other Member may use public telecommunications transport networks and services for the movement of information within and across borders, including for intra-corporate communications of such service suppliers, and for access to information contained in data bases or otherwise stored in machine-readable form in the territory of any Member."[31]

That said, relying entirely on intergovernmental discussions may not be the most rapid and effective ways to arrive at solutions supporting the objective of an open Internet. A public-private track of analysis and structured input to the process would seem a necessary complement to the effort. It would be especially helpful if such an effort could be pursued in a multistakeholder manner that draws in expertise from the Internet community, a point we return to below.

In the meanwhile, as the Doha Round has trundled along to wherever it is now, the various mega-regional initiatives have adopted or are in the process of adopting a number of provisions of direct relevance to our concerns here. The problem, of course, is that the prospects for their ratification or completion are at best very cloudy, with large-scale opposition growing and leading politicians backing away from them in ways that will be difficult to reverse. In the end, it may be that these provisions will need to be incorporated into other processes conducted in a more open and multi-stakeholder manner. Either way, it is useful to briefly review what has been achieved.

Leaving aside the more controversial bits pertaining to intellectual property protection, as well as the good language on customs duties, non-discrimination and the like, three articles of the TPP are of particularly direct relevance to our discussions:

> *Article 14.8: Personal Information Protection*
> 1. The Parties recognize the economic and social benefits of protecting the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce.
> 2. To this end, each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce. In the development of its legal framework for the protection of personal information, each Party should take into account principles and guidelines of relevant international bodies.
> 3. Each Party shall endeavor to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction.
> 4. Each Party should publish information on the personal information protections it provides to users of electronic commerce, including how:
> (a) individuals can pursue remedies; and
> (b) business can comply with any legal requirements.
> 5. Recognizing that the Parties may take different legal approaches to protecting personal information, each Party should encourage the development of mechanisms to promote compatibility between these different regimes. These mechanisms may include the recognition of regulatory outcomes, whether accorded autonomously or by mutual arrangement, or broader international frameworks. To this end, the Parties shall endeavor to exchange information on any such mechanisms applied in their jurisdictions and explore ways to extend these or other suitable arrangements to promote compatibility between them.

> *Article 14.11: Cross-Border Transfer of Information by Electronic Means pp.*
> 1. The Parties recognize that each Party may have its own regulatory requirements concerning the transfer of information by electronic means.
> 2. Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person.
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.
>
> *Article 14.13: Location of Computing Facilities*
> 1. The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.
> 2. No Party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory.
> 3. Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.[32]

While it is still evolving and is less elaborate, the relevant TiSA language also merits consideration. With the pending national edit suggestions in brackets removed, we have an Article 2 that would be called either "Movement of Information" or "Cross-Border Information Flows," and which basically holds that, ""No Party may prevent the transfer, access, processing or storing of information (including personal information) outside that Party's territory if conducted in connection with a business."[33] The provision on personal information is of course not settled; Korea wants the cross-border data transfers of service providers to be based on "informed consent," and negotiators appear to be rather divided on Article 4, Personal Information Protection, with no edits having been suggested by the United States. Similarly, Article 9 on either "Local Infrastructure" or "Local Presence" is heavily bracketed, and the treatment of financial services is very much up in the air, but the core principle proposed by the United States is that,

> No Party may require a service supplier, as a condition for supplying a service or investing in its territory, to:
> (a) use computing facilities located in the Party's territory;
> (b) use computer processing or storage services supplied from within the Party's territory; or
> (c) otherwise store or process data in its territory.[34]

Finally, the eventual treatment of these issues in the TTIP seems unclear based on the leaked documents available to me; perhaps others in the group can shed light on the state of play. And to be complete, it should be noted that the the US–South Korea free trade agreement provides for free cross-border information flows and encourages the parties to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders.

In sum, we seem to be in a difficult situation where there is a pressing need to stem the tide of localization and TDF restrictions that are contrary to Internet openness and an evolution toward a more dynamic environment for wealth creation and innovation. But the trade policy mechanisms available to us are moving at less than Internet speed and, in some cases, facing a realistic prospect of failure. The question then is how to take forward the important work that has been done so far in a manner that will be more politically viable.

Here it is useful to return to an issue raised in the Introduction to this paper: the orientation towards international trade agreements of the institutionalized global Internet community. As noted, we not talking here about the sort of anti-globalization, anti-capitalist, anti-trade civil society activists that are familiar to trade policy makers. In general, the Internet community is anything but this. However there is a widespread distrust of closed intergovernmental processes making decisions that could impact Internet freedom in any manner. The procedural model of trade policymaking is simply diametrically opposed to the sort of open multi-stakeholder processes that they are used to engaging in when making decisions about such matters us the management of Internet core resources and questions pertaining to the Internet freedom and human rights. Moreover, on substantive grounds, many are strongly opposed to treating data protection and personal privacy in a trade policy context, and tend to regard the sort of intellectual property provisions typically included in trade agreements as unduly restrictive of users' freedom.

For many years, the Internet community showed significant disinterest in the workings of international trade policy. During the World Summit on the Information Society process of 2002 to 2005, efforts to promote awareness of the role of the WTO in the Internet context generally fell on deaf ears. This situation remained largely unchanged until last year when the news of the TPP and other mega – regional negotiations became widespread, alas through leaks. Now there is quite a bit of mobilization underway, and the fact that texts like the TPP contain provisions that are supportive of an open Internet does not sway opinions due to larger perceptions of the process.

One notable example here is the multi-stakeholder Open Digital Trade Network. Spearheaded by the Electronic Frontier Foundation, a long-time and very influential advocate for online civil liberties, the network grew out of a meeting held in February of this year that adopted a *Brussels Declaration on Trade and the Internet.* The Declaration reads in part,

> 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.[35]

Signatories to this statement included such radical 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, while not a signatory to the document, the i2Coalition 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."[36] This coalition comprises over eighty 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 that was chaired by former Swedish Prime Minister Carl Bildt released at report called *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 favor 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.[37]

Finally, trade agreements also will figure prominently at this year's meeting of the IGF at Guadalajara in November. After much debate, it was decided to hold a Main Session on *Trade Policy and the Internet* to assess the issues in a plenary-type setting. The IGF will also feature workshops on *Aligning Multistakeholder Norms and the Digital Trade Agenda, Trans-Pacific Partnership: Good or Bad for the Internet?,* and *Meet TISA: The Trade Agreement You've Probably Never Heard Of.*[38] There were also a number of similar workshop proposals that were rejected for various reasons, but in general it can be expected that the processes and substance of the agreements discussed above will be subject to some tough multistakeholder scrutiny and often depicted as impinging on Internet governance processes that are organized in a very different manner.

In short, the search for trade solutions to data localization and barriers to TDF may get caught up in the wider socio-politics of trade in general and trade and the Internet in particular. How quickly progress can be made and relief can provided to the companies and other stakeholders effected is far from clear. Whether in the meanwhile the spread of such policies would contribute to the spread of Internet fragmentation is also a concern. As such, while the trade processes move along at their respective speeds, it maybe worth pursuing parallel opportunities to promote Internet openness.

One option to consider may be better use of intergovernmental "soft law" agreements. The range and diversity of these has increased in in recent years at the same time that treaty-making has become a notably more difficult enterprise. Indeed, the Internet governance environment has become increasingly thick with such normative frameworks in recent years. Of course, those who feel that only binding agreements backed up by the possibility of sanctions really matter often disparage the value of declarations, recommendations, memorandums of understanding and the like. But norms, properly leveraged, can be powerful things. Once parties have agreed to a formulation, monitoring and pressure may be brought to bear in ways that yield real results. One problem is that this follow-up is often rather uneven. Here, bringing in a multistakeholder dimension can be helpful. As the trade lawyer Joost Pauwelyn has noted,

> Especially at the international level where centralized enforcement is absent, actors comply for reasons other than or beyond legal constraint (e.g. reputation, reciprocity, retaliation, prior consent to or perceived legitimacy of the norm in the first place…to the extent informal rules or mechanisms include, and are the result of a consensus amongst, not only diplomats or central state representatives, but also state or non-state actors more closely connected to the trade problem and required implementation (e.g. regulators, custom officials, public agencies, regional authorities, businesses or NGOs), achieving prompt compliance with informal rules may be easier."[39]

There are certainly some possible starting points available. One is the somewhat dusty OECD TDF declaration of 1985 that declared governments' intent to promote access to data and information and related services, and to avoid the creation of unjustified barriers to the international exchange of data and information. Perhaps this could be refreshed? Moreover, the September 2016 G20 summit in China agreed on the need to "Clarify the application of existing GATS commitments to cross-border data flows. Develop provisions to discourage local data storage requirements, while recognizing legitimate public interests such as privacy and financial regulation."[40] In addition, the governments said:

> G20 members recognize that freedom of expression and the free flow of information, ideas, and knowledge, are essential for the digital economy and beneficial to development, as reaffirmed in paragraph 4 of the Tunis Commitment of WSIS. We support ICT 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.[41]

Further, the May 2016 G7 summit in Japan agreed that "We continue to support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to access online information, knowledge and services of their choice. We oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives."[42] And in a somewhat less artfully stated manner, the Joint Declaration by G7 ICT Ministers added that, "We continue to support ICT policies that preserve the global nature of the Internet, promote the flow of information across borders and allow Internet users to access online information, knowledge and services of their choice. We oppose data localization requirements that are unjustifiable taking into account legitimate public policy objectives."[43]

One would think that these and similarly framed statements by major world powers could be built upon through the kind of multistakeholder engagement suggested by Pauwelyn, above. And one could even imagine trying to constitute not only a multistakeholder add-on to intergovernmental processes, but a parallel track of multistakeholder dialogue and problem solving that would complement such efforts. In this regard, the various experiences of the Internet community in managing critical resources through institutions like ICANN, the IETF and the RIRs might be worth considering to see what could be learned from them and applied elsewhere. Or less ambitiously, informal issue-networks, or what a commission led by Estonian President Toomas Ilves called "distributed governance groups," could perhaps offer a more decentralized and flexible approach.[44]

Arguably, to sustain such efforts, what may be needed is a new multistakeholder community of expertise and practice that could inch the issues forward on a consensual basis and with broader public support. If one thinks back to the 1980s, we experienced something similar with the development of a so-called "epistemic community" for international trade in services. This community brought together trade policy experts, reformist telecommunications analysts, TDF experts and others from across governments, stakeholder groups and the research community to constitute a transnational community based on shared principled and causal beliefs.[45] These actors often were able to directly influence the ideas being institutionalized in nascent policy processes taking place in the GATT, OECD and other forums. Ultimately, they helped to define some of the core concepts underlying the GATS architecture, and were particularly important in reimaging telecommunications as a traded rather than jointly provided service that plays a key dual role in services trade. That many of the actors involved had no direct material interests in the outcomes of the negotiations lent additional credence to the ideas they put on table and the agenda shaping they provided.

One wonders it would be desirable to develop a similar epistemic community on data localization and flow in order to advance Internet openness, including through trade disciplines. Arguably, failure to engage the diverse stakeholders in the Internet community would not only be a missed opportunity to draw in useful expertise, but also could lead to the entrenchment of more robust and diverse sentiment against trade solutions.

In light of the above, a few items the workshop might wish to consider include:

1. What are the main substantive and political challenges involved in assessing the coverage of data localization and flow issues by governments' GATS schedules of commitments?

2. How can we best elaborate a shared baseline to assess whether localization and TDF barriers are, per the TPP provisions, 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 on the use or location of computing facilities greater than are required to achieve the objective? Is it best to leave this to a dispute

settlement process to sort out, assuming the TPP becomes a reality? Would an expert multistakeholder dialogue on these matters be a useful complement to the slow wheels of trade machinery?

3. More generally, would it be useful to more systematically explore the options for using soft law arrangements and multistakeholder processes as a means of moving reasonably quickly and building broader public support?

Conclusion

During the remainder of the year, a White Paper could be assembled that would be akin to the Internet fragmentation paper released at Davos in January 2016. It could provide a landscape survey of the problems of localization and barriers---their causes, forms, incidence, etc.---and of relevant efforts in the trade and other governance environments to provide some measure of order and relief to the impacted parties. As indicated, the apparent lack of systematic information about the scope of the phenomena may require some creativity to fill out the picture, perhaps to include structured and anonymized interviews with companies about the challenges they have encountered, the results of which could be presented in a typology or in small box-type case studies. Suggestions on this and other potential approaches would be very helpful.

In parallel with the research effort, it would be useful to organize a process of community dialogue. WEF participants could provide input to the written work in response to a draft version of the paper. Perhaps they could engaged in online dialogue in a dedicated platform to build consensus and clarify any differences of view. This would help to advance both the research and any action oriented-work undertaken following the Annual Meeting. Ideally, we would bring together thought leaders from difference stakeholder groups who may have different starting points but through dialogue find common ground on the substantive and procedural issues in play. More ambitiously, perhaps at some point the WEF might consider employing the sort of Task Force approach we used to produce recommendations on the global digital divide to the G7 summit at Okinawa in 2000. A multi-stakeholder task force that brought together both Internet constituencies and the trade community with academics and governmental participation might be able to advance creative and efficacious recommendations.

Finally, a more long-term thought on the knowledge gaps mentioned above: The WEF's annual Global Information Technology Reports present a Networked Readiness Index used to rank countries, which includes a 1st "Political and regulatory environment" pillar. While the metrics used are at a higher level of aggregation than specific policies, perhaps it would be possible to try and captures our issues through this mechanism. Alternatively, an intergovernmental organization may be well suited to conducting surveys and otherwise gathering evidence so that the international community is better able to identify and address the issues.

[1] Drake, William J., Vinton G. Cerf and Wolfgang Kleinwächter, 2016. *Internet Fragmentation: An Overview,* The World Economic Forum, January. Available at www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf; Meltzer, Joshua P., 2016. *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. Available at http://e15initiative.org/publications/maximizing-opportunities-internet-international-trade.

[2] Tuthill, L. Lee, 2016. "Cross-border Data Flows: What role for Trade Rules?" in, Research Handbook on Trade in Services, edited by Pierre Sauvé and Martin Roy, Edward Elgar, forthcoming, p.4.

[3] Manyika, James, Jacques Bughin, Susan Lund, Olivia Nottebohm, David Poulter, Sebastian Jauch, and Sree Ramaswamy, 2014. *Global Flows in a Digital Age: How Trade, Finance, People, and Data Connect the World Economy.* McKinsey Global Institute, April, p.1. Available at, http://www.mckinsey.com/insights/globalization/global_flows_in_a_digital_age.

[4] Manyika, James, Susan Lund, Jacques Bughin, Jonathan Woetzel, Kalin Stamenov, and Dhruv Dhringra, 2016. *Digital Globalization: The New Era of Global Flows*. McKinsey Global Institute, March, p.1. Available at, http://www.mckinsey.com/business- functions/mckinsey-digital/our-insights/digital-globalization-the- new-era-of-global-flows.

[5] Pepper, Robert, John Garrity, and Connie LaSalle, 2016. "Cross-Border Data Flows, Digital Innovation, and Economic Growth," in *The Global Information Technology Report 2016: Innovating in the Digital Economy,* edited by Silja Baller, Soumitra Dutta, and Bruno Lanvin, The World Economic Forum, pp. 39-40. Available at https://www.weforum.org/reports/the-global-information-technology-report-2016.

[6] For an assessment of the synergistic effects of breakthrough advances in digital, physical and biological technologies, see, Schwab, Klaus. 2016. *The Fourth Industrial Revolution,* The World Economic Forum.

[7] Bradley, Joseph, Joel Barbier and Doug Handler, 2013. "Embracing the Internet of Everything To Capture Your Share of $14.4 Trillion," Cisco. Available at https://www.cisco.com/web/ciscocapital/apjc/assets/pdfs/IoE_Economy.pdf.

[8] See, Drake, William J. 2000. "The Rise and Decline of the International Telecommunications Regime," in *Regulating the Global Information Society,* edited by Christopher T. Marsden, Routledge, pp. 124-177. Available at, http://tinyurl.com/wjdrake-regime-2000.

[9] International Telecommunication Union, 2015. *Collection of the Basic Texts Adopted by the Plenipotentiary Conference,* ITU, p. 43. Available at http://www.itu.int/pub/S-CONF-PLEN-2015.

[10] For a longitudinal and cross-sectoral review of the evolution of international communications regimes and the role of sovereignty therein, see, Drake, William J., 2008. "Introduction: The Distributed Architecture of Network Global Governance," in, *Governing Global Electronic Networks: International Perspectives on Policy and Power*, edited by

William J. Drake and Ernest J. Wilson III, The MIT Press, pp. 1-78. Available at http://tinyurl.com/wjdrake-ggn-2008.

[11] Gassman, Hans-Peter and G. Russell Pipe. 1976. "Synthesis Report," in *Organization for Economic Cooperation and Development, Policy Issues in Data Protection and Privacy: Concepts and Perspectives---Proceedings of the OECD Seminar 24th to 26th June, 1974*, Organization for Economic Cooperation and Development, p. 27.

[12] Quoted in Drake, William J. 1993. "Territoriality and Intangibility: Transborder Data Flows and National Sovereignty," *Beyond National Sovereignty: International Communications in the 1990s,* edited by Kaarle Nordenstreng and Herbert I. Schiller, Ablex, pp. 259-313. Available at http://tinyurl.com/wjdrake-tbdf-1993.

[13] See, Organization for Economic Cooperation and Development, 2013. "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers, No. 229,* OECD Publishing. Available at http://dx.doi.org/10.1787/5k3xz5zmj2mx-en

[14] In 1983, a consulting house surveyed fifty one American-based TNCs, thirty four of which had endorsed the OECD Guidelines. Of the thirty four, only ten said they were doing anything at all to comply with European data protection, and top executives of ten were completely unaware that their firms had even endorsed the agreement. See, Business International Corporation, 1983. "Transborder Data Flows: Issues, Barriers and Corporate Responses," Business International Corporation.

[15] See, United Nations Centre on Transnational Corporations, 1983. *Transborder Data Flows and Brazil,* United Nations; and United Nations Centre on Transnational Corporations, 1982. *Transnational Corporations and Transborder Data Flows: A Technical Paper,* United Nations.

[16] Intergovernmental Bureau of Informatics,1984. "Second World Conference on Transborder Data Flow Policies: Working Document," Intergovernmental Bureau of Informatics, November, pp. 47-48.

[17] Organization for Economic Cooperation and Development, 1985. "Declaration on Transborder Data Flows," available at: http://www.oecd.org/sti/ieconomy/declarationontransborderdataflows.htm

[18] US International Trade Commission, 2014. *Digital Trade in the U.S. and Global Economies, Part 2. Publication 4485, Investigation No. 332-540*, US International Trade Commission, August, p. 81. Available at www.usitc.gov/ publications/332/pub4485.pdf.

[19] For a good survey of these forms, see, Force Hill, Jonah, 2014. "The Growth of Data Localization Post-Snowden: Analysis and Recommendations for U.S. Policymakers and Industry Leaders," *Lawfare Research Paper Series,* 2, 21 July. Available at, https://lawfare.s3-us-west-2.amazonaws.com/staging/Lawfare-Research-Paper-Series-Vol2No3.pdf.

[20] "Iran Begins Roll Out of 'National Internet,'" *CircleID,* 29 August 2016. Available at http://www.circleid.com/posts/print/20160829_iran_begins_roll_out_of_national_internet.

[21] Available at http://businessroundtable.org/ sites/default/files/reports/BRT%20PuttingDataToWork.pdf.

[22] Chander, Anupam and Uyen P. Le, 2015. “Data Nationalism”, *Emory Law Journal,* v. 64, pp. 721-722. Available at http://law.emory.edu/elj/_documents/volumes/64/3/articles/chander-le.pdf.

[23] For an initial effort to estimate the macroeconomic costs, see, Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel, and Bert Verschelde, 2014. “The Costs of Data Localisation: Friendly Fire on Economic Recovery”, *ECIPE Occasional Paper No. 3.*, European Centre for International Political Economy. Available at http://www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf.

[24] Castro, Daniel, 2013. “The False Promise of Data Nationalism”, The Information Technology & Innovation Foundation, December, p. 1. Available at http://www2.itif.org/2013-false-promise-data-nationalism.pdf.

[25] For discussions, see, Drake, William J., and Kalypso Nicolaïdis, 2000. “Global Electronic Commerce and GATS: The ‘Millennium Round’ and Beyond,” in *GATS 2000: New Directions in Services Trade Liberalization,* edited by Pierre Sauve and Robert M. Stern, The Brookings Institution, pp. 399-437. Available at http://tinyurl.com/wjdrake-gatsgac-2000; and Sacha Wunsch-Vincent, *The WTO, the Internet and Trade in Digital Products: EC-US Perspectives,* Hart Publishing, 2006.

[26] United States of America, 2016. “Work Programme on Electronic Commerce---Non-Paper from the United States,” JOB/GC/94, 4 July, pp. 2 & 1. Available at https://www.wto.org/english/news_e/news16_e/good_14jul16_e.htm.

[27] Burri, Mira, forthcoming. "The WTO as an Actor of Global Internet Governance", in, *Global Internet Governance Institutions: Multistakeholder, Multilateral, and Beyond,* edited by William J. Drake and Mira Burri, Cambridge, p.11. Available at https://www.wto.org/english/news_e/news16_e/good_14jul16_e.htm http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2792219.

[28] Quoted in, Weber, Rolf H. and Mira Burri, 2013*. Classification of Services in the Digital Economy*, Springer, pp. 75-76.

[29] Crosby, Daniel, 2016. *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, p. 10. Available at http://e15initiative.org/publications/analysis-of-data-localization-measures-under-wto-services-trade-rules-and-commitments.

[30] Meltzer, Joshua, 2016. *Maximizing the Opportunities of the Internet for International Trade*, p. 20.

[31] World Trade Organization, 1994. Annex on Telecommunications. Available at https://www.wto.org/english/tratop_e/serv_e/12-tel_e.htm.

[32] Trans-Pacific Partnership, 2015. "Chapter 14: Electronic Commerce," pp. 14-5 to 14-7. Available at https://www.mfat.govt.nz/assets/_securedfiles/Trans-Pacific-Partnership/Text/14.-Electronic-Commerce-Chapter.pdf.

[33] Trade in Services Agreement, undated. "Annex on [Electronic Commerce]," p.2. Available at https://wikileaks.ch/tisa/ecommerce/05-2015.

[34] *Ibid.,* p.7.

[35] https://www.eff.org/files/2016/03/15/brussels_declaration.pdf.

[36] https://www.i2coalition.com/support-goals-brussels-declaration-trade.

[37] Global Commission on Internet Governance, 2016. *One Internet,* Centre for International Governance Innovation and Chatham House, p. 78. Available at https://www.ourinternet.org/report.

[38] Session descriptions are available at http://www.intgovforum.org/cms/igf16-workshops/igf2016-workshops-evaluation-results.

[39] Pauwelyn, Joost, 2014. "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* 17, pp. 745 & 747. Available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2474525.

[40] G20, 2016. "Reinvigorating Trade to Support Growth: A Path Forward," Note for Ministers and Governors for the July G-20 Ministerial Prepared by IMF Staff, September, p. 5. Available at http://www.g20.org/English/Documents/Current/201608/P020160815370397652241.pdf.

[41] G20, 2016. "G20 Digital Economy Development and Cooperation Initiative," September, pp. 3-4. Available at http://www.g20.org/English/Documents/Current/201609/P020160908736971932404.pdf.

[42] G7, 2016. "Principles and Actions on Cyber," May, p. 2. Available at http://www.mofa.go.jp/files/000160279.pdf.

[43] G7, 2016. "Joint Declaration by G7 ICT Ministers," May, p.3. Available at http://www.japan.go.jp/g7/_userdata/common/data/000416959.pdf.

[44] The Panel on Global Internet Cooperation and Governance Mechanisms, 2014. *Towards a Collaborative, Decentralized Internet Governance Ecosystem,* May. Available at https://www.icann.org/en/system/files/files/collaborative-decentralized-ig-ecosystem-21may14-en.pdf.

[45] For a detailed account, see, Drake, William J., and Kalypso Nicolaïdis. 1992. "Ideas, Interests and Institutionalization: 'Trade in Services' and the Uruguay Round," in *Knowledge, Power and International Policy Coordination*, a special issue of *International Organization,* edited by Peter Haas, 45, pp. 37-100. Available at http://tinyurl.com/wjdrake-tis-1992.