WORLD ECONOMIC FORUM

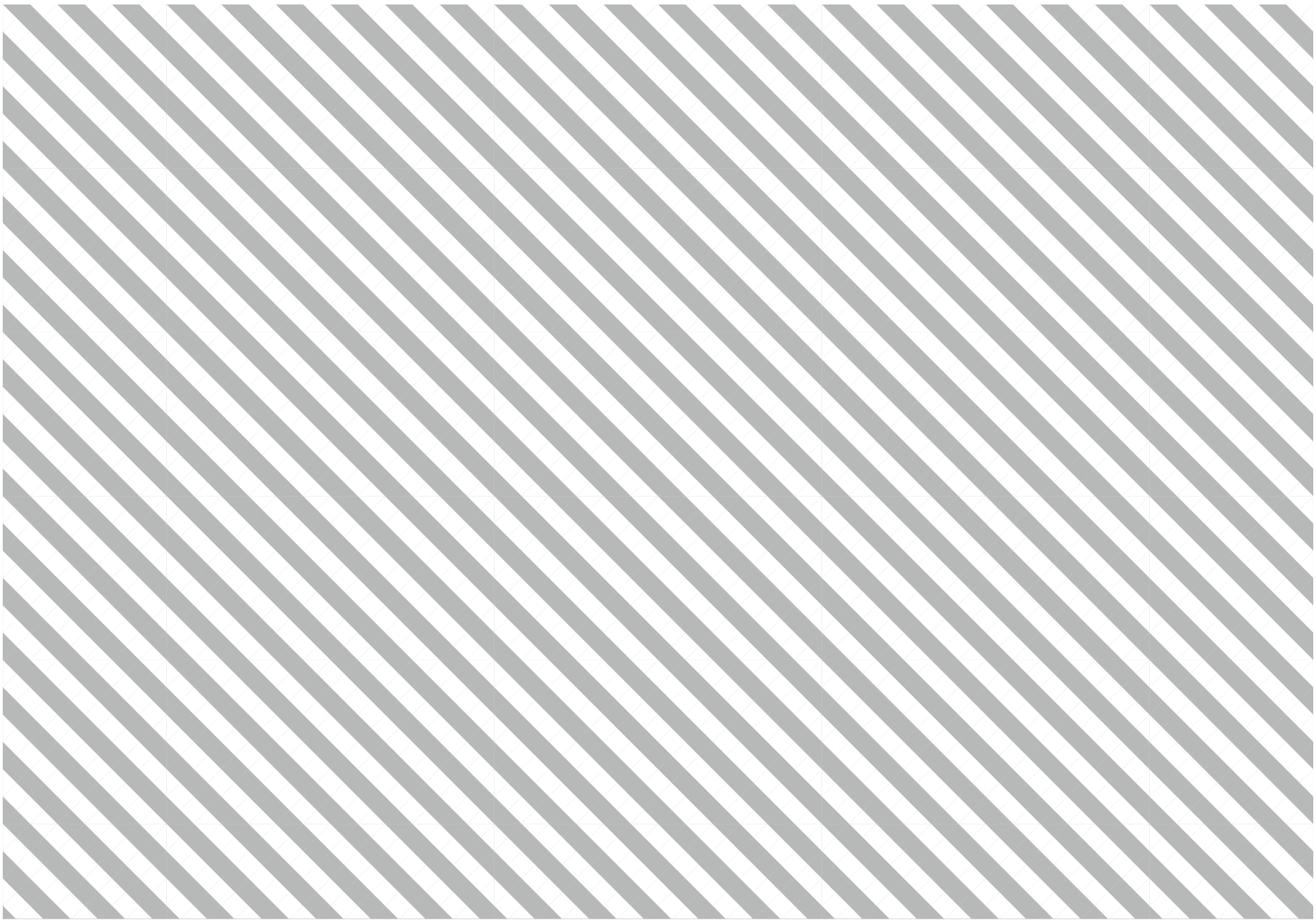
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Exploring International Data Flow Governance

Platform for Shaping the Future of Trade and Global Economic Interdependence

December 2019



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
Email: contact@weforum.org
www.weforum.org

Contents

Foreword 5

Chapter 1: Regulating cross-border data flows – domestic good practices 7

- The context 7
- On data flow restrictions 7
- What happens at home: domestic examples 10
- What data flows enable 13
- Ways forward: good practices 16

Chapter 2: Trade policy and data flows – progress to date and future innovations 18

- The challenge 18
- State of play 18
- Future rule innovations 21
- Regulatory good practice 22
- International standards 22
- Policy interoperability 23
- Adequacy, mutual recognition and equivalence 23

Conclusion 25

Contributors 27

Endnotes 28

Foreword

Richard Samans, Managing Director

Kimberley Botwright, Community Lead, International Trade and Investment

The World Economic Forum's Platform for Shaping the Future of Trade and Global Economic Interdependence is organizing a global multistakeholder discussion aimed at deepening understanding and expanding common ground on one of the most dynamic and challenging policy issues of our time: cross-border data flows.

The two chapters presented in this World Economic Forum white paper have been developed to prepare the ground for this discussion. They were written by four distinguished co-authors and have benefited from the input of an expert group composed of private-sector, think-tank and academic leaders from around the world.

The paper provides an overview of current domestic policy approaches and international trade frameworks related to data flows. This baseline analysis is intended to be a useful resource for all stakeholders, including domestic and international economic policy-makers.

The white paper considers "data" in a broad sense, without limiting the analysis to any specific data classification. Further, it considers data flow "restrictive measures" broadly, including but not limited to data localization policies. This approach recognizes that the cross-border elements of countries' data rules vary – in other words, whether or not the data can be moved abroad and under what conditions depends on the structure of the relevant legislation.

At the global level, data flow considerations need to be untangled from those relating to competition and taxation frameworks. These debates may be interrelated, but the tools to address them are not necessarily the same. If used interchangeably, they may be ineffective. The aim of this publication is to understand how countries can satisfy policy objectives in such domains as privacy, cybersecurity, financial system safety and so on with the least restrictive effect on trade and global value chains.

The first chapter analyses the primary ways in which countries typically regulate data flows at the domestic level and examines the restrictive effect of such measures. It then explores what commercial and other values data flows enable in the economy and society and why the search for simpler approaches may be worth pursuing. It concludes with a series of suggested good practices governments can use to strike a suitable balance between the free flow of data needed to support a modern and productive open economy, on the one hand, and the protection of personal information, assurance of adequate levels of cybersecurity and integrity of law enforcement procedures, etc. on the other.

The second chapter provides an overview of relevant trade policy tools and principles at the multilateral and plurilateral or bilateral levels. It explores new approaches that could be used to achieve greater regulatory interoperability and reduced friction between jurisdictions on essential topics affecting data flows.

The chapter concludes that trade policy should combine regulatory cooperation with market-enabling commitments in respect of data flows. Failure to do so could result in countries using trade agreement exceptions – an important part of the trade architecture intended to preserve policy space and autonomy – merely to justify restrictive approaches. Regulatory cooperation can help address the underlying policy concern giving rise to restrictions directly, ensuring that it will be satisfactorily addressed by the jurisdiction receiving the data.

Further thought and discussion on how the growing preference of countries to regulate data flows can be reconciled with the essential role these now play in the functioning of so many aspects of our economies is warranted. Informal, multistakeholder discussion among experts and practitioners from governments, business, academia and civil society could help to lay the foundation for wider agreement on practical solutions in this regard. The World Economic Forum looks forward to facilitating such a process during 2020 in cooperation with the Government of Japan as part of the follow-up to the G20's Data Free Flow with Trust discussions that took place earlier this year.

The Platform for Shaping the Future of Trade and Global Economic Interdependence provides space for informal, public-private cooperation on important integration policy and practical challenges. Stakeholders work together to shape soft law and other multistakeholder advances. Efforts are also underway to improve trade and investment facilitation as well as sustainable value chain operations through industry best practices and cooperation. Collaboration with business, civil society and policy-makers is achieved through informal discussion, knowledge integration and partnerships. A network of 30 leading policy research institutes and international organizations anchors these efforts.

This paper is part of a platform project to help governments develop frameworks for trade in increasingly digital-driven economies. The project explores the actions required to ensure that opportunities from emerging technologies enable small and medium enterprises (SMEs) and entrepreneurs in developing economies and drive more inclusive trade. It also encourages discussion on how to navigate potential disruptive effects to ensure digital trade drives inclusive growth.

Chapter 1: Regulating cross-border data flows – domestic good practices

Anupam Chander, Professor of Law, Georgetown University
Martina F. Ferracane, Research Associate, European Centre for International Political Economy

The context

Individuals, business and machines are generating enormous international flows of data in what has been, to date, a readily global digital economy. Governments, in response, are grappling with the interplay between these international data flows and domestic policy objectives related to privacy, consumer protection, economics, cybersecurity, national security and law enforcement.

Without a clear, consistent path towards achieving legitimate policy objectives and maximizing the benefits of the digital economy, governments have increasingly opted for approaches that restrict data flows. Trust between policy-makers – in other words, confidence that a domestic policy objective will be met even if data flows out of a jurisdiction – on these sensitive topics is too often quite low. In particular, concerns over law enforcement needs, the abuse of data, the difficulty of taxing the digital economy, escalating cyberattacks, unfair competition and a need for control are driving a restrictive approach.

Yet it is not clear how different types of data flow restrictions contribute to tackling these important policy issues, and perhaps policy measures that are less restrictive of trade could be more effective. In addition, these relatively new virtual borders are increasingly disrupting the world wide web and jeopardizing service supply and choice, value chain integration and essential innovations that might otherwise be of great significance for humanity.

Are these restrictions necessary, or can domestic policy objectives be achieved while still maintaining access to the varied benefits of global information flows? The "data free flow with trust" model conceptualized by Japanese Prime Minister Abe at the World Economic Forum Annual Meeting 2019 offers the world a vision that it is possible, and more effective, to meet domestic policy objectives while allowing data to flow across borders. Recognizing that "cross-border flow of data, information, ideas and knowledge generates higher productivity, greater innovation, and improved sustainable development",[1] G20 trade and digital economy ministers in June 2019 committed to promoting both respect for domestic and international laws and frameworks for interoperability throughout various regulatory regimes. In the Osaka Declaration on the Digital Economy released alongside the Japanese G20, leaders representing 45 economies affirmed the importance of national and international policy discussions to harness the full potential of data and the digital economy.[2]

Further consensus and confidence-building are needed, however, on what a "less" restrictive or "more" facilitative approach looks like and whether it is workable. An approach that both embraces data flows and protects regulatory objectives will probably require greater regulatory cooperation, which governments can pursue through bilateral, regional and international settings, such as the Organisation for Economic Co-operation and Development (OECD), the G20, the Asia-Pacific Economic Cooperation (APEC) forum or the Association of Southeast Asian Nations (ASEAN) Economic Community (AEC).

Trade agreements, whether at the World Trade Organization (WTO) or in preferential arrangements, can include commitments that encourage a balance between domestic policy objectives and the economic gains of data flows. Trade policy has experience of achieving such a balance to enable both international goods and services supply within a domestic regulatory framework. Trade policy has fewer tools, by comparison, for determining specific standards for governing data. Discussions ongoing at the OECD and G20 to reform current international tax principles relevant to the digital economy, meanwhile, may address public revenue-related issues that are sometimes tied up in data flow debates.

Progress on global agreements can be challenging in practice. Trade policy options are covered in Chapter 2, below, where they are linked to international efforts in this area. This first chapter offers context on several domestic regulations influencing cross-border data flows to date. It also highlights techniques for developing such legislation. These approaches, in turn, are more likely to encourage international collaboration and, hopefully, increase the overall trust, economic gains and societal benefit from the digital economy.

On data flow restrictions

Countries are introducing policies on the transfer of data to achieve various objectives, either by mandating companies to store data within certain borders or by imposing additional requirements for data to be transferred abroad.[3] Restrictions on data flow have increased dramatically in the past decade, though not all types of data are necessarily subject to these measures, with scope varying between countries and contexts.[4] It is estimated that today there are more than 200 data regulations being implemented worldwide[5] and the overall level of restrictiveness as measured in the European Centre for International Political Economy (ECIPE)'s Data Restrictiveness Index has doubled over the past decade.[6]

These policies can be imposed by local, central or regional governments, or in certain cases also by a single public entity, such as hospitals. As a result, different types of data may be subject to specific regimes for cross-border transfers, creating a "spaghetti bowl" of requirements for entities to navigate. Several taxonomies exist for classifying how cross-border data transfers are regulated worldwide.[7] For the purpose of this chapter a brief overview is provided as follows:

1. Unconditional flow regime: Data can flow freely across borders without specific requirements.

2. Conditional flow regime: Data cannot be transferred abroad unless certain conditions are fulfilled by the recipient country, the data controller and/or data processor. Such a regime has to date typically been applied to personal data.

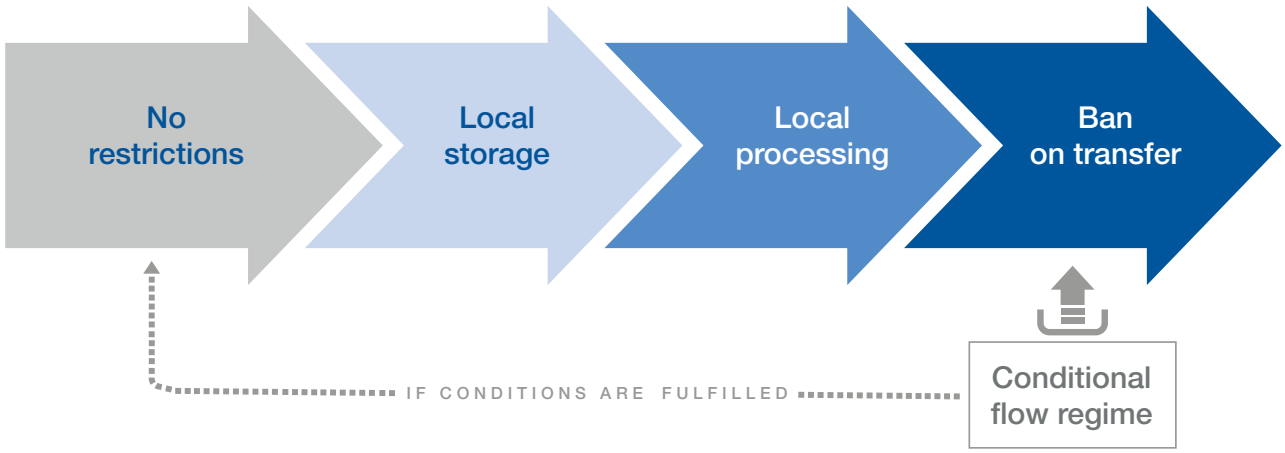
3. Local storage requirement: Certain data cannot be transferred across borders unless a copy is stored within the borders of the jurisdiction. This type usually applies to certain tax and accounting records, corporate documents, public archives, and user data held by telecommunication companies or other internet intermediaries.

4. Local processing requirement: The main processing of the data must be performed in data centres located in the implementing country. The company must either build or lease a data centre in the country, or switch to local providers of data processing solutions. Such an approach is sometimes taken with respect to data held by public authorities or in sensitive sectors such as finance, health and telecommunications.

5. Ban on data transfers: Data must be stored, processed and accessed within the territory of the implementing country. This type differs from local processing in that the company is not allowed even to send a copy of its data abroad. It usually applies to data classified as especially sensitive, such as healthcare data or financial data.

Figure 1 summarizes these types, from least to most restrictive. As shown, for a conditional flow regime, data can flow freely if the conditions are fulfilled, while otherwise the data may be restricted from being transferred abroad.

Figure 1: Different regimes on cross-border data flows



Source: Ferracane (2017).

Data flow restrictions can impose costs on firms not only in the digital sector but in virtually any sector of the economy, as well as on research institutions and in academia and civil society.[8] Specific evidence of the range of costs and benefits of data flow restrictions is, however, still relatively scarce. Insights currently available on economic costs, employment, cybersecurity, productivity and privacy protection are summarized below.

Some studies assess how restrictions affect immediate economic activity – for example, by limiting imports of services, leading to reduced choice and availability for domestic industries.[9] When data restrictions apply, local companies are not free to use the most convenient data processing provider, and may have to pay for more expensive, or even duplicate, services when transferring data, including perhaps daily business activities, such as human resources management. One study found that local companies could face costs of 30–60% more for their computing needs if restricted from transferring data abroad.[10]

Limited services access and higher data processing costs could end up broadly affecting countries' ability to compete in the Fourth Industrial Revolution, within which growth will be driven by technology deployment. Low levels of global economic integration suggest that data restrictions in some smaller developing economies may not yet have a major impact on domestic firms.[11] Yet data restrictions will probably result in opportunity costs for future integration or limit entrepreneurs from employing the most innovative global services.

Logically, the economic costs of data flow restrictions apply not only in the home market but also affecting trade partners. Anecdotal evidence from a study of Indian firms showed that, for two-fifths of those surveyed, the compliance costs with the EU General Data Protection Regulation (GDPR) (a draft earlier version at the time of this study) could result in lost commercial opportunities of more than $10 million, while, for another third, losses were expected to be between $1 million and $10 million.[12]

For some policy-makers, amid the fierce competition of global markets, data restrictions seem to offer one way to guarantee local job creation for the digital era. However, studies examining the impact of localization on employment opportunities, whether in IT or technical vocations, tend to find limited gains. Findings suggest data centres typically contain expensive high-tech equipment that is imported, with construction generating short-term work, but few full-time staff in the long run.[13] Jobs associated with data centres have also decreased sharply as such centres become more automated in advanced and developing economies alike.[14]

Setting economic costs aside, for many companies the biggest effect of data restrictions is hindrance of cybersecurity measures. Local data infrastructure providers may lack the resources and skills to implement high security standards, thereby putting data at greater risk of a breach. Localization also increases entry points, thereby reducing overall security, and is a major concern for sectors such as financial services. Data restrictions may also make it more difficult to use global cloud solutions, with their various security advantages.[15]

Conversely, a focus on localizing data processing can detract attention from cybersecurity defensive measures, since data security is not a function of where data is held but how it is maintained. Defensive measures can include technological solutions reliant on data flows (such as automated updates, hardware-based security, encrypted data and multifactor authentication), as well as innovations in operations – user education and awareness through training and certificates, creation of computer emergency response teams (CERTs) and use of the cyber kill chain.[16] On the policy side, useful efforts include data breach notification laws, international coordination and conventions, education curricula and liability rules.[17]

Companies that are forced to keep data locally may have less oversight on their operations.[18] Anti-money laundering (AML) efforts, for example, rely on service providers staying one step ahead of global criminal activity. Analysing data patterns can help, while market segmentation weakens these efforts.

Keeping data locally may not be necessary for lawmakers' own oversight. With regard to financial service providers, the Global Financial Markets Association (GFMA) notes that financial institutions can ensure government access to data regardless of where the data is stored.[19] Indeed, the Financial Stability Board (FSB) warned, in a June 2019 G20 report, of the negative impact of restrictions on data transfers, which may actually undermine regulators' ability to perform their supervisory role.[20] These actors need access to relevant information to monitor risk exposures and market function effectively.[21] Further, different privacy laws or data restrictions can result in conflicts of law for multinational firms subject to multiple regulatory reporting regimes. Strict regimes on data transfers could also result in firms removing financial services from certain markets, hampering financial inclusion along the way.[22]

Discussion of privacy by design – and, more generally, the use of privacy-enhancing technologies – is relevant in this context because it provides valuable solutions to protect data privacy regardless of the location of data.[23] After the Snowden revelations,[24] two important standardization

bodies for internet protocols, the Internet Architecture Board (IAB) and the Internet Engineering Task Force (IETF), have turned to privacy by design, which had originally been outside of their scope. The global nature of these protocols may offer a broader alternative to localization.[25]

Data restrictions at scale are a relatively new phenomenon. The available evidence suggests that restrictions may not be the most suitable option to achieve a suite of intended policy objectives. While restrictions may result in benefits for one country or firm, the same may not hold true more generally, requiring some of the broader influences cited above to be considered. Use of a restrictive measure merits careful economic, legal and technical analysis, as well as discussion with stakeholders and society on the trade-offs. The impacts of restrictions on economies of different levels of development has not been studied comprehensively, probably due to limited evidence, and merits further investigation.

Figure 2: Is data the new oil?
An emerging analogy suggests that data is the new oil and should thus be protected as a kind of valuable national resource. We consider arguments for and against this proposition below.

Yes	No
Valuable insofar as it is important to economic development	Oil is inherently valuable, while most data has almost no inherent value, though it is important to many individuals how their data is treated.
Tradeable as a commodity	Oil maintains value, while data's value diminishes rapidly over time.
	Oil can be used broadly, while data is less broadly useful.
	Oil is rivalrous, while data is non-rivalrous. One person's use of data does not diminish others' benefit from that data; benefits can be shared.

What happens at home: domestic examples

Domestic regimes on data flows vary, even while many of the relevant debates and concerns may be similar. The variation can be an expression of different societies' preferences concerning the treatment and use of data. These preferences may be expressed by a majority or minority, implicitly or explicitly debated, and may change over time.

Figure 3 provides one illustration for each of the data flow restrictions in the taxonomy developed in Figure 1 above. These examples and a few others are elaborated below in relation to the law's stated primary objective(s).[26] In some instances, objectives may overlap, or the priority may not be clear, or an undisclosed motive is the real driver. This section is not intended as a comprehensive regulatory mapping, rather it offers a snapshot of different approaches taken to date with varying degrees of restrictiveness.

Figure 3: Regulation illustration of regimes

Regime	Regulation
No restrictions	EU's Regulation on Non-Personal Data (regulation on intra-EU data flow)
Conditional flow regime	EU's privacy law – GDPR
Local storage	Vietnam's 2018 Cybersecurity Law[27]
Local processing	Russia's 2015 Data Protection Law
Ban on transfer	Australia's My Health Records

Personal data protection

Personal data protection is among the objectives that are most likely to involve a data restriction. Russia's 2015 Data Protection Law requires the storage of personal data of residents within the country.[28] Its digital development and communications ministry has clarified that information can be stored abroad in a "secondary" database, subject to cross-border data transfer rules. Thus, rather than a ban on data transfer, this is a local data processing regime and relatively restrictive. The regime offers three main options for foreign transfer: (1) to countries that are signatories to the Council of Europe's Convention for the Protection of Individuals With Regard to Automatic Processing of Personal Data (Convention 108); (2) to countries it recognizes as having adequate protections; or (3) with prior written consent of the data subject.[29]

The European Union (EU)'s GDPR, the bloc's main privacy protection mechanism, offers several options for moving personal data outside the European Economic Area (EEA). Chapter 5 of the GDPR specifies that personal data can flow to non-EEA countries that the European Commission declares offer an adequate level of protection – a list that currently includes Argentina, Canada, Israel, New Zealand, Switzerland and Japan. In addition, the EU-US Privacy Shield mechanism allows US companies certifying compliance with certain rules to transfer European residents' personal data to the US. For countries not yet declared adequate, a series of other options is outlined for entities to move European personal data abroad. Entities can agree to standard contractual clauses (available to all companies) or binding corporate rules (available for transfers only among corporate affiliates), in either case as approved by the appropriate authorities.[30]

The GDPR also contemplates transfers under codes of conduct or certification mechanisms, though no such processes are in place thus far (however, note that an EU Cloud Code of Conduct has been submitted for approval under the GDPR). According to anecdotal evidence, larger multinational entities rely on binding corporate rules (BCRs) for intra-company transfers, but adequacy could be helpful for transfers to non-affiliates, and in reducing administrative and other costs for those without BCRs, such as small businesses.

Brazil's new Data Protection Regulation (LGPD), which will come into force in August 2020, follows a model relatively similar to the GDPR. Personal data may be transferred under nine listed circumstances. The GDPR establishes the procedures and elements to be considered by the European Commission when assessing data adequacy, while the LGPD is as yet not fully specified. Singapore offers yet another approach to personal data transfer, permitting an entity transferring data to demonstrate "comparable protection" abroad as the standards of Singapore's Personal Data Protection Act of 2012.

To facilitate personal data transfer in a way that meets their citizens' expectations, some countries allow the use of "transfer mechanisms". Australia, Chinese Taipei, Singapore and the Philippines have recently adopted the Asia-Pacific Economic Cooperation (APEC) forum Cross-Border Privacy Rules (CBPR), joining the US, Mexico, Canada, Japan and South Korea – a type of transfer mechanism further discussed in Chapter 2 below. Notably, it works in conjunction with the APEC Privacy Framework, a set of guiding principles for business on common privacy issues. Each country adopting the CBPR system must have a privacy enforcement authority in place to investigate and enforce its obligations. Countries can agree to this system unilaterally, but the CBPR system is available to the 21 APEC states.

Non-personal data

Another recent EU regulation, applicable as of 28 May 2019, seeks to remove obstacles to the flow of non-personal data within the bloc.[31] This regulation aims to encourage more data flows throughout the EU, supporting the establishment of a competitive data economy by creating a larger market. The mandate, however, is limited to free flow within the EU, and not with other countries or regions.

Globally, while policy-makers have focused more on personal data, restrictions on the flow of non-personal data is a concern for some multinational businesses that move such data extensively for day-to-day operations, or businesses that work with large datasets. Some firms note, however, that it can be challenging to separate personal from non-personal data.[32] These complexities escalate due to different jurisdictions adopting different definitions of personal and non-personal data, which may cause overlaps between the two types of data.

Law enforcement

Existing legal methods of ensuring government access to data stored overseas are burdensome and slow. Electronic privacy laws such as those in the US sometimes prevent companies from sharing information with foreign governments, even where the foreign government is investigating a local citizen with respect to a local crime.[33] Governments have failed to provide sufficient resources for mechanisms implementing existing mutual legal assistance treaties, despite the enormous increase in cross-border evidence requests. Some stakeholders expect restrictions on data flows to be used by policy-makers as an alternative response.

The US Clarifying Lawful Overseas Use of Data (CLOUD) Act, passed in 2018, eases law enforcement access to data between countries with which the US has reached an executive agreement; however, it requires more procedures from the government authority seeking access and provides additional safeguards for foreign residents. The first such agreement was signed by the US and the UK in October 2019. Ensuring law enforcement access to data is a less restrictive approach to data transfers that also achieves the other policy objective at hand.

As an alternative model, the EU Law Enforcement Directive provides a mechanism for data transfer by EU states for law enforcement purposes by competent authorities within the EU.[34] While it permits the free movement of such data within the EU, it establishes strict conditions for data transfer for law enforcement purposes to outside governments. These include transfers based on adequacy, or binding contracts in the absence of an adequacy ruling. European states are implementing the directive through national laws, in contrast to the GDPR, which as a regulation has binding legal force throughout the bloc.

Security

China's Cybersecurity Law, effective since 2017, imposes a ban on the transfer of data abroad (with limited exceptions) with respect to personal as well as "important" data on operators of "critical information infrastructures". To date, the Chinese government has issued draft guidelines only for the law, which many businesses consider has complicated compliance efforts. It remains unclear what constitutes a critical information infrastructure, though draft guidelines reference energy, finance and transportation, as well as large social media and e-commerce enterprises. Draft guidelines with respect to "personal information" proposed in 2019 by the Cyberspace Administration of China would require prior regulatory approval before transfer of personal information outside China.[35]

Viet Nam's Cybersecurity Law follows a similar path, requiring foreign companies providing telecommunications or internet services in Viet Nam to store data about Vietnamese users locally, to establish a local office and to perform a security assessment prior to any cross-border data transfer.[36]

Most states do not require a cybersecurity review before transfer abroad. A simpler approach to cybersecurity goals could be to promote risk-based cybersecurity standards, such as the International Organization for Standardization (ISO), which offer a means to establish cybersecurity protections regardless of the location of the data.

At a regional level, in 2014, African Union member states adopted the African Union Convention on Cyber Security and Personal Data Protection (the Malabo Convention) which encourages signatories to establish legal frameworks protecting personal data and principles to include in these frameworks. It also covers obligations on cybersecurity measures to be taken at a national level. Thus far, however, only five states have ratified the Convention. Regional approaches to issues such as cybersecurity can particularly help countries developing regulatory capacity for the digital economy.

Financial service supervision

The Reserve Bank of India implemented data localization obligations for payment providers in 2018 to ensure access for supervisory purposes.[37] Some worry, conversely, that this obligation will reduce the information needed by global fraud systems and complicate cybersecurity efforts.[38]

Brazil considered adopting a local processing requirement for services used by financial institutions to ensure system security. Policy-makers eventually opted for a different approach, set forth in the Brazilian Central Bank Regulation no. 4658/2018, which outlines rules for hiring cloud computing services, data processing and storage and cybersecurity policies. The regulation covers all financial institutions authorized to operate by the Central Bank. It allows for the use of foreign services, irrespective of data centre location, while outlining several requirements. The latter include the existence of an information exchange agreement between the Brazilian Central Bank and the regulatory authorities of the service provider.

South Korea, going further, has loosened regulations to permit financial services institutions to use foreign cloud services as well as other outsourced services. The changes remove the requirement for regulatory approval before outsourcing of information technology services by financial institutions and permit them to use their own contracts with certain obligatory terms rather than a standardized preapproved contract form.[39]

Health data privacy

Australia's My Health Records Act of 2012 (Section 77) prohibits the storing or processing of personally identifiable health records outside the country. The US, meanwhile, permits the transfer of health information abroad, but requires consideration of such things as increased hacking prevalence as part of an information security risk assessment.[40] The EU has no special limitations with respect to the export of health data, treating it like other personal data for the purposes of cross-border transfer; health data is, however, considered sensitive personal data, and the transfer of personal data is carefully regulated, as we have noted.

What data flows enable

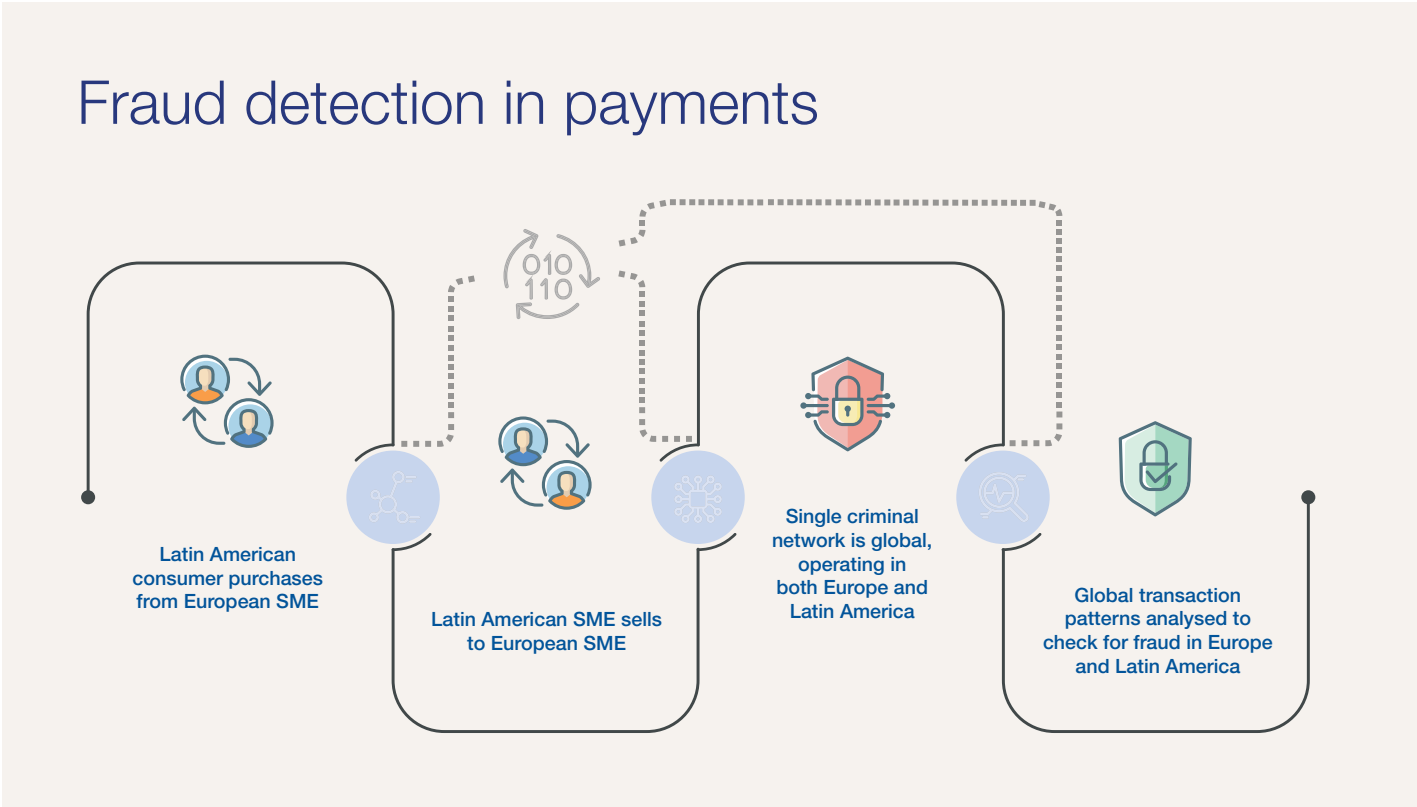
It may be helpful at this stage to review what data flows enable and why the search for simpler approaches might be worth pursuing. Data flows are often described as the lifeblood of the modern economy. These flows include different types of information – from video streaming, social media and financial data to business services and machine sensor data. Businesses increasingly depend on data flows for interconnected machinery, big data analytics, back-office consolidation, supply-chain automation, digital collaboration and cloud scalability.[41] Data flows are often an integral part of new technologies such as smartphones, the internet of things (IoT), artificial intelligence (AI), cloud computing, the app economy, outsourcing of services, e-commerce, big data, digital streaming, social media and the sharing economy.[42]

Where possible, data flows may also enable scientific advances, such as through the aggregation of anonymized health datasets for research[43] or to gather accurate data to benchmark progress on the United Nations Sustainable Development Goals (SDGs).[44] An explosion of data sources in the natural environment from advanced sensors, to take another specific example, can translate into new knowledge on conservation. Several initiatives combine data gathered from automatic identification system transponders on large ships – required to avoid accidents – to predict commercial fishing behaviour in real time and help law enforcement protect natural habitats.[45]

Much of contemporary trade in services would not exist without cross-border data flows.[46] According to the latest WTO World Trade Report, services trade has been the most dynamic component of global exchange for the past decade, expanding at a rate of 5.4% per year on average. Services exports generate jobs, while services trade more generally can improve firms' competitiveness. Although developing economies trade much less in services, WTO estimates that if new digital technologies are adopted, their share in total global services trade could increase by 15% in the coming decades.[47]

Figure 4: Illustrations of global data flows

Note: These graphics depict hypothetical situations.



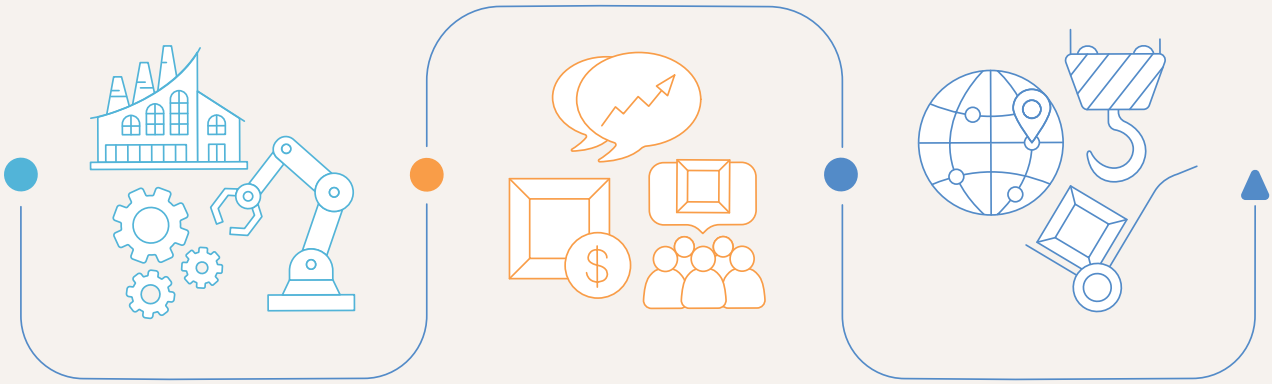
Source: World Economic Forum

Smart farming

Using global command centres, service providers monitor crop and soil sensors, controlling drones and other connected farm equipment across the world, increasing agricultural productivity, while reducing water, fertilizer and pesticide use.

Source: World Economic Forum

SMEs and global value chains

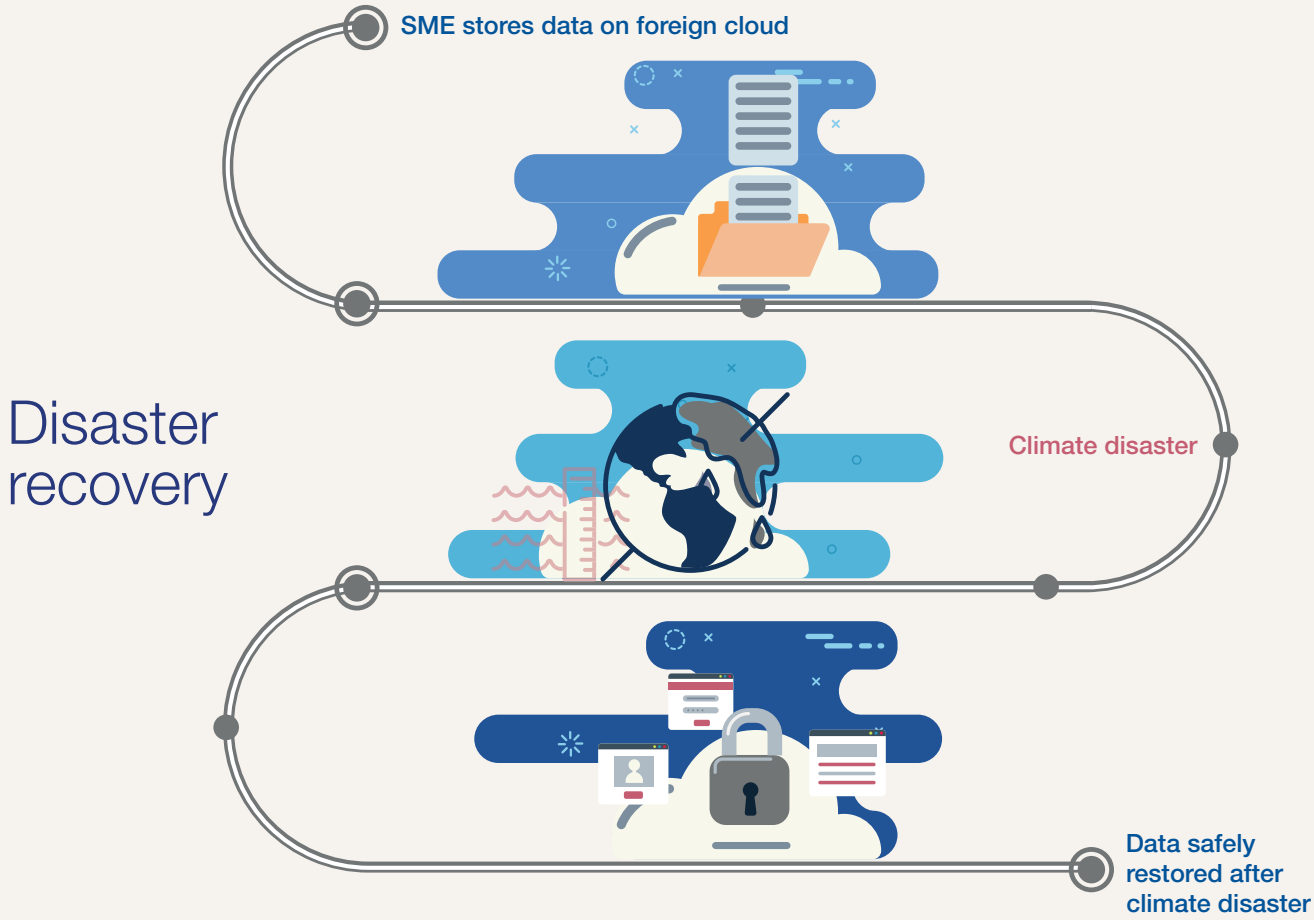


American MNC buyer

Supply chain compliance

African SME seller

Relies on data flows to Europe for certification of quality, as well as labour and environmental protections



Source: World Economic Forum

Global marketplace

Ways forward: good practices

Many stakeholders agree that data flows are critical for the economy, for innovation and, increasingly, for sustainable development. Information has always been vital to human advancement. In today's digital age more than ever, though, societies must debate how to use and treat data while determining consent for and ensuring safety of this information at personal and national levels. Then, in a globalized world, the challenge is to ensure that the regulatory manifestation of societies' answers to these questions are attended to between different jurisdictions and preferences. These are the critical "trust" issues linked with data governance and data flows.

The pursuit of a less restrictive or "facilitative" approach can ensure the continued benefits and inclusiveness of data flows, while other policy tools, such as those on taxation and competition, will be important to ensure overall system equity and sustainability. Rather than significantly curtailing cross-border data flows, policy-makers could work towards alternatives. As noted in the introduction to this chapter, that would probably involve greater trust-building and regulatory cooperation between governments. But much can already be done at the domestic level to pave the way or at least facilitate such collaboration.

Domestic policy-makers may wish to consider that it need not be a zero-sum game between allowing for data flows and achieving legitimate policy objectives. Rather, they may wish to explore regulation that balances free flow with arrangements that protect personal information, promotes cybersecurity standards and supports efficient government law-enforcement access procedures consistent with due process. Drawing from the above discussion, as well as recent research, the following are some emerging techniques along these lines for consideration:

1. Policy-makers could clearly identify intended objectives (e.g. to improve data privacy and ensure proper collection of tax revenues) and engage in a technical analysis to ensure that any restriction on cross-border data flow is necessary and proportionate to achieve the desired policy objective.[48] Allowing different stakeholders to provide inputs to the analysis, including technical experts, civil society and businesses, would bring insights on how to achieve policy goals while reducing harms caused by restrictions. The analysis can also help ensure compliance with existing trade law obligations.

2. In addition to a technical analysis, governments could estimate the economic costs of compliance with a measure for both local and foreign companies, with special consideration of employment and effect on small and medium enterprises. Doing so might help determine lower-cost options to achieve a given policy objective. Such analysis could also call for comments from all stakeholders on potential broader costs from a given measure, such as reduced cybersecurity, hampered financial inclusion, innovation drag, limited service provider choice and so on.

3. Multistakeholder discussions should be framed within a transparent regulatory procedure, with consultations during the regulatory development and the possibility for different domestic and foreign actors to provide technical and economic evidence on the effect of the measure being considered and suggest possible alternatives that might be more effective to achieve the stated policy objective. A transparent discussion will allow governments to separate the risks of transferring data abroad from the risks connected to transferring data to third parties in general and whether or not the scope of the measure (the sector and data covered) is proportionate to achieve the desired policy objective.

4. When governments determine that a certain restriction on cross-border data flows is needed and is the least restrictive option available, they should ensure that the measure is transparent and non-discriminatory for local and foreign entities and provide clarity to enable compliance. In this context, "transparency" could be judged based on the availability and clarity of information on the measure, advance notice on the implementation of the changes, clarity on the sanctions and enforcement and so on. Where appropriate, policy-makers could notify policies within regional or international forums for facilitating foreign business compliance and provide sufficient time and consideration for public comment.

5. Harmonizing domestic privacy and cybersecurity frameworks on regional or where available international standards can increase compliance while reducing costs. Examples are the APEC CBPR rules regarding data protection, ISO 27701 and the US National Institute of Standards and Technology (NIST) framework[49] for cybersecurity, which enable companies to transfer data without restrictions, if appropriate protections are in place and the companies remain accountable. Measures promoting the adoption of privacy and security by design should also be encouraged. The approach may help reduce compliance burden, raise trust in the system and make regulatory cooperation on data governance easier to pursue.

6. When restrictions on cross-border data flows are imposed, policies should include transfer mechanisms that enable compliance for entities looking to transfer data abroad under certain conditions. Policy-makers may wish to go beyond an "individual consent" approach, to include transfer mechanisms that are more systemic. These are likely to be more micro, small and medium-sized enterprise (MSME) and development-friendly from a sheer implementation perspective. Examples include adequacy findings, BCRs, seals and certificates,[50] standard contractual clauses (SCC) and the adoption of certification mechanisms agreed between relevant policy-making counterparts, such as the APEC CBPR or the EU-US Privacy Shield.[51]

7. Governments should consider steps to facilitate MSME compliance. Some of the transfer mechanisms cited above remain, in practice, expensive to use. Implementation is important from a privacy perspective, but may lie beyond the capacity of some entities, leading to non-compliance. More thinking is needed on transfer mechanisms that are inclusive. In the ASEAN, for example, work under the ASEAN Framework on Digital Data Governance to build interoperability with the APEC CBPR system, but also tailored to suit regional needs, is ongoing. Policy-makers should explore mechanisms that are practical for MSMEs.

8. Governments should enforce their privacy and cybersecurity law in a fair and impartial manner. Enforcement capacity is a critical feature of cross-border data flow with trust. Domestic openness to work with regional enforcement agencies for privacy and cybersecurity standards may also be encouraged, such as the EU (already in existence for personal data under GDPR) and ASEAN (currently considering regional enforcement systems).

9. Wherever possible, policies should eliminate obstacles to the flow of non-personal data. One example of this approach is the EU Regulation on Free Flow of Non-Personal Data.

10. Governments should increase regulatory cooperation with other governments on consumer protection, law enforcement access to data, cybersecurity and privacy, noting that many countries might require technical and financial resources to monitor firms' behaviour outside their borders. Such cooperation should also include assistance to least developed countries to build a stronger overall global data system. Organizations, such as United Nations Conference on Trade and Development (UNCTAD) eTrade for All, provide a one-stop shop for initiating assistance requests by countries.

Countries can shape domestic legislation on cross-border data flows that enables and facilitates global information exchange while protecting important regulatory goals. Data flows may themselves even be critical for achieving certain domestic regulatory goals, including increasing participation in trade in services and strengthening the digital economy. Chapter 2 discusses how international trade principles might reinforce such approaches.

Policy-makers will only be able to pursue this path, however, if domestic rules allow for that possibility. Well-crafted provisions that include options for collaboration with others would provide the roots from which a more trusted, secure and efficient international architecture may eventually grow. Policy-makers should also consider the implications of restrictions on data flows, not only on trade and development, but also on the functioning of the internet, human rights (including freedom of expression) and global communication.

Chapter 2: Trade policy and data flows – progress to date and future innovations

Abdelhamid Mamdouh, Senior Counsel, King & Spalding
Joshua P. Meltzer, Senior Fellow, Global Economy, Brookings Institution

The challenge

As Chapter 1 highlights, just as the opportunities offered by data flows and digital technologies are growing, governments are increasingly regulating in ways that restrict information movement since commercial tensions between nations have flared up in relation to technology dominance, cybersecurity, abuse of personal information, tax receipts and control of the digital space. Critically, international trade rules and the WTO adjudication system are already strained, and unlikely in their current forms to withstand a full-blown tech or "data usage" war.

As Figure 1 illustrates, international data flow restrictions come in various forms domestically. This chapter summarizes international trade policy's approach to data flows and suggests potential further steps to consider. Trade policy needs to grapple with how it should interface with this emerging data governance. Negotiators need to consider what trade policy can do and where it can most helpfully be part of a broader perspective on international collaboration, including facilitating some of the techniques highlighted in Chapter 1. Amid today's fraught geopolitics, this is not only a question of trade rules "staying relevant" but also about using available policy tools effectively to avoid harmful outcomes.

The WTO General Agreement on Trade in Services (GATS) contains disciplines relevant to data flow across borders for the purpose of supplying services. Greater understanding regarding the scope and technical details of these disciplines is much needed. A group of 80 WTO members is engaged in e-commerce negotiations, which include data flows among other issues.

Several preferential trade agreements (PTAs) have ventured further into specific rules for cross-border data flows – notably, the CPTPP (Comprehensive and Progressive Agreement for Trans-Pacific Partnership) agreed between 11 Pacific-Rim nations and the pending USMCA (United States-Mexico-Canada Agreement). Data flow commitments in these deals are complemented by improved market access for services (including financial services) and a commitment to avoid data localization requirements, subject to tailored exceptions.

Even these provisions, however, may fall short of securing a conducive environment for data flows or limiting international fallout over data control. The actors involved must have confidence that allowing data to cross borders will not undermine other policy objectives, that data will be protected according to domestic standards and that governments may have appropriate access to data if needed. Without this trust, governments are likely to rely heavily on trade agreement "exceptions" provisions to justify data flow restrictions, which may well be for legitimate domestic policy purposes.

Trade and other policy-makers may wish to spend time considering how to encourage further international regulatory cooperation on data. Doing so could reduce the reliance exceptions a core part of trade policy architecture, and instead increase trust between policy-makers to obviate the need for data flow restrictions.

State of play

At the WTO, apart from a handful of obligations (mainly most favoured nation [MFN] and transparency), GATS disciplines apply only to services sectors in which members have undertaken specific commitments. The modest level of commitments currently scheduled under GATS limits the scope of application of such disciplines in practice. Except for those members who acceded to the WTO after its establishment in 1995, most members made commitments during the "Uruguay Round" negotiations (1985–1994) that established the global trade body as it is known today. WTO members should nonetheless recall a few foundational aspects of the GATS.

The GATS can apply to any government measure that "affects" trade in services, be it directly or indirectly. That would include any data flow restriction that affects the supply of a service covered by the Agreement, noting that the MFN (Article II) and transparency obligations (Article III) apply to all services, while market access, national treatment and additional commitments apply only in sectors where a WTO member schedules commitments.

It should also be noted that the GATS considers services to be "products". Members have been guided by the United Nations Central Product Classification (CPC) system in scheduling their commitments. The GATS as a legal instrument is also considered by many to be technologically neutral. This view stems from the fact that the Agreement does not contain any provisions that distinguish between the different technological means used in supplying a service. A banking service is the same "product" whether it is supplied in person or through mobile technology.

Trade in services is defined as the supply of services through four "modes".[53] The GATS defines "supply" broadly to include "the production, distribution, marketing, sale and delivery of a service".[54] Unlike trade in goods, which takes place post-production, trade in services typically starts with the production of a service throughout the value chain and ends with the delivery of the service to the consumer. Government measures relating to cross-border data flows for the purpose of supplying services at any stage of the supply chain are covered by GATS obligations.

WTO members each list market access and national treatment commitments for sectors. A WTO member's market access commitment in a given sector is a commitment not to maintain any of the six types of restrictive measures, mostly of a quantitative nature, identified in Article XVI of the GATS, subject to any scheduled limitations. A commitment with no limitations covers all six types of measures in their discriminatory and non-discriminatory forms.[55] This has implications for some forms of data flow restrictions. For example, where a full mode 1 (cross-border) commitment is made on computer and related services, but the cross-border flow of relevant data is restricted, that would be deemed a restriction on the supply of the service and would be inconsistent with the market access commitment.

A WTO member's national treatment commitment requires that no measures are maintained that discriminate, either *de jure* (by law) or *de facto* (in practice), against foreign services or suppliers, subject to any limitations as explicitly entered in the schedule.[57] Therefore, any regulatory measure relating to data flows such as data localization requirements must provide no less favourable treatment to foreign services and suppliers than that given to domestic "like" suppliers. For example, any additional cost of local data processing or storage requirements that adversely affect the competitive position of foreign service suppliers compared to their counterparts of national origin would be inconsistent with a national treatment commitment. Even if such a requirement applies equally to suppliers of national origin (formally identical treatment), it would still be inconsistent with a national treatment commitment if it *de facto* affects the competitive position of a foreign supplier. The rule applies subject to any scheduled limitations in the sector concerned.

Members can also make additional commitments, beyond market access and national treatment, under GATS Article XVIII. The approach is designed to allow members to negotiate new disciplines in areas where additional rules are needed and where market access and national treatment commitments would not be sufficient to address the regulatory issues affecting trade. Additional commitments regarding data flows could go a long way in clarifying or improving existing GATS rules.

Service suppliers listed in a WTO member's schedule also benefit from an explicit obligation on data flows in the GATS Annex on Telecommunications.[58] The Annex requires WTO members to ensure that foreign service suppliers in committed sectors may use basic telecommunications networks for the movement of digitized information within and across borders, including for intra-corporate communications of such service suppliers and for access to information contained in databases in the territory of any member. Furthermore, given how critical data flows are for the supply of services, the same provision requires that any new or amended measure that significantly affects such use be notified to the WTO and be subject to members' consultation.

Another explicit obligation on data flows is found in paragraph 8 of the Understanding on Commitments in Financial Services, which requires members – where commitments have been scheduled according to the Understanding – not to take any measure that would prevent the transfer of financial data by electronic means. Obligations and commitments related to data flow may, in some cases, conflict with a country's other policy objectives. As is standard in trade agreements, the GATS contains specific provisions allowing WTO members to deviate from obligations and commitments. It contains exceptions in four categories: general exceptions, security exceptions, the prudential exception (specific to the financial sector) and exceptions relating to the security and confidentiality of messages. Figure 4 outlines these in further detail. However, and as will be explained, failure to address the underlying drivers of data flow restrictions will probably lead countries to rely heavily on exception provisions to justify their ongoing use. As a result, in addition to commitments on data flows, international regulatory cooperation is needed to reduce the regulatory incentive to restrict cross-border data flows in the first instance.

Disciplines on recognition

Notwithstanding the MFN obligation in Article II, Article VII of the GATS allows members to recognize the education or experience obtained, requirements met, or licences or certifications granted in a particular country, for the purposes of the fulfilment of its own standards or criteria for the authorization, licensing or certification of service suppliers. This licence to differentiate in the treatment of service suppliers coming from different foreign jurisdictions is subject to a very important requirement that a member granting recognition must not discriminate between service suppliers of different members in the application of the substantive standards according to which recognition is being granted. In other words, there must be one set of substantive criteria according to which recognition is granted.

Article VII provides that recognition may be granted autonomously or through mutual agreement between the members concerned. However, it stipulates that other members are to be afforded the opportunity to demonstrate that they fulfil the requirements for recognition – be it mutually or autonomously.

The Annex on Financial Services also contains a provision of a similar nature regarding prudential regulation.

Figure 5: Exceptions under GATS

General exceptions

Article XIV of the GATS (General Exceptions) provides legal cover for a WTO member to use a measure inconsistent with its obligations or commitments in order to protect a list of public policy objectives, including public morals, public order, public health, prevention of fraudulent practices and privacy of individuals, several of which are relevant to cross-border data flows.

This provision does not specify the type of measures a member may take. The Article lists the objectives that may be protected as mentioned above – and the conditions that the member adopting the measure must observe. It stipulates at the outset that the measure in question must not constitute a means of "unjustifiable discrimination" or a "disguised restriction on trade in services". It also requires that the measure in question must be "necessary" for the protection of the respective objective. Since the policy objectives are explicitly identified, the necessity test does not question the objective, nor the level of its attainment intended by the policy-maker, it only examines the measure.

The security and confidentiality of messages

There are two exceptions in the GATS for the specific purpose of protecting the security and confidentiality of messages. The first is found in paragraph 5 (d) of the Annex on Telecommunications, which provides that, notwithstanding the obligations relating to cross-border data flows, a member may take any necessary measures to ensure the security and confidentiality of messages, subject to requirements and caveats similar to those found in Article XIV.

The second similar exception is found in paragraph 8 of the Understanding on Commitments in Financial Services. While this paragraph establishes the obligation to allow the transfer of information and financial data, it also provides that this does not restrict the right of a member to protect personal data, personal privacy and the confidentiality of individual records and accounts. This provision does not contain a necessity test. However, like the prudential exception, it requires only that such a right should not be used to circumvent the provisions of the Agreement.

Security exceptions

Article XIV *bis* of the GATS (Security Exceptions) addresses national security concerns. A WTO member shall not be required to furnish any information that it considers contrary to its national security, and a member shall not be prevented from taking any action that it considers necessary for the protection of its essential security interests.

This Article specifies the type of situations in which the security exception may be invoked but does not contain caveats as found in Article XIV, most notably, neither a "necessary" requirement, nor that it must not constitute arbitrary or unjustifiable discrimination or a disguised restriction on trade.

The prudential exception

The GATS Annex on Financial Services includes an exception that is specific to that sector. Members shall not be prevented from taking measures for prudential reasons. It does not specify the type of measures that may be adopted. It elaborates on "prudential reasons" with an indicative list of such objectives, namely "the protection of investors, depositors, policy holders or persons to whom a fiduciary duty is owed by a financial service supplier, or to ensure the integrity and stability of the financial system". The prudential exception does not require a necessity test, but rather that a measure must not be used as a means of avoiding commitments or obligations under the Agreement.

GATS disciplines on data flows, as such, could ensure that members do not restrict cross-border data flows for the supply of services. However, as applied, their effectiveness is less than satisfactory. As noted, apart from the general obligations of MFN and transparency, these disciplines apply only where a WTO member has made commitments. Further, most members' commitments were scheduled in 1994 according to an outdated classification (UN CPC Provisional released in 1991).[59] The CPC has been revised repeatedly to capture the technologically driven evolution of services products. For example, the addition of a section under Chapter 84 of CPC version 2.1 (the latest CPC version, released in 2015) covers "online content services" that are often referred to as "digital products". Outdated commitment classification is another weakness in GATS relevance to data flows. Future changes to schedules would need to account for latest classification developments. The discrepancy between older commitments and newer definitions has been flagged by some WTO members.

Some PTAs address data flows more directly. The CPTPP and USMCA include broad commitments to the free flow of information across borders and measures prohibiting forced location of computing facilities, with accompanying exceptions provisions.[60] These commitments exist alongside an obligation for parties to maintain legal frameworks on personal information protection. The 2019 US-Japan Digital Trade Agreement includes similar data flow and computer location commitments, modelled on USMCA.

The EU-Japan PTA includes a commitment to transfers of financial information for the business of a financial service supplier[61] subject to prudential exceptions.[62] However, for other non-financial data flows, the parties merely agree to reassess the issue of free flow of data within three years.[63] Elsewhere, the Pacific Alliance has agreed to consider a data flows provision, while Australia and Singapore have updated their bilateral PTA e-commerce chapter to reflect the CPTPP commitments.

Recently, Singapore, New Zealand and Chile have commenced negotiations on a Digital Economy Partnership Agreement, including focus on issues such as the cross-border transfer of information, location of computing facilities, wider trust environment on encryption, cybersecurity, safe and secure online environment and digital identities. Additionally, in October 2019 Australia and Singapore announced scoping discussions for a Digital Economy Agreement, with official negotiations expected to be launched soon.

As seen, financial services can experience slightly different treatment on data flows in PTAs. In the CPTPP financial institutions and cross-border financial services, suppliers are carved out from an e-commerce chapter that includes data flow and data localization commitments. The CPTPP financial services chapter does contain a rule that parties must allow information transfer in electronic or other form for business purposes,[64] but it does not include a prohibition on forced data localization. These commitments in the e-commerce and financial services chapters are subject to exceptions.

An updated approach to data flows in the USMCA financial services chapter includes a commitment to the free flow of information as well as a prohibition of data localization requirements, subject to appropriate exceptions.[65] The prohibition against data localization is subject to the party's financial regulatory authorities, for regulatory and supervisory purposes, having immediate, direct, complete and ongoing access to relevant information used by a covered person outside its territory. Before imposing data localization, the parties also commit to providing a reasonable opportunity to covered entities to remediate any lack of information access. The US-Japan Digital Trade Agreement combines the USMCA digital trade chapter commitments and those found in the financial services chapter into a single commitment on data flows to all sectors (including financial services) and replicates the USMCA prohibition on data localization found in the digital trade chapter and the analogous provision in the financial services chapter, ensuring that every sector is covered by these important provisions.[66]

Future rule innovations

Horizontal data flow commitments – as modelled in some PTAs – may offer an important signal to markets on the future direction of data regulation. Yet, until policy-makers have confidence that allowing data to leave their jurisdiction will not undermine domestic regulatory goals, there will remain a strong incentive to restrict data flows.[67] Countries with relevant trade commitments may resort to exceptions, while those without these commitments will not be encouraged to sign up to new deals, rendering trade policy commercially redundant on this topic.

As such, new trade rules may also wish to consider encouraging regulatory good practices and cooperation to build trust between jurisdictions, especially in specific use cases such as cybersecurity and privacy. Building bridges between countries' regulatory systems to minimize trade costs is not a new approach. Indeed, the OECD identifies 11 forms of international regulatory cooperation, integration, specific negotiated agreements, regional agreements, mutual recognition agreements (MRAs), requirements to consider standards and recognition of standards.[68] The following section summarizes ideas relevant to data flows from Meltzer (2019),[69] as well as ideas generated by a World Economic Forum Trade Policy and Data Flows Expert Group, and builds on Chapter 1.

Regulatory good practice

Encouraging regulatory "good practice" has been an increasing trend in PTAs.[70] The approach could be applied, whether at multilateral or PTA level, to data flow governance to render it more facilitative. Elements to consider include transparency of regulatory procedure, consultation during regulatory development and advance notice of regulatory changes.[71]

The CPTPP and USMCA offer insights into the trend, though similar approaches are now common in other PTAs. The CPTPP's regulatory coherence chapter includes a provision on "core good regulatory practices" and its environment chapter includes several pledges to undertake public consultation for the implementation of measures, while the financial services chapter recognizes the importance of transparent regulations and the requirement to publish any proposed regulation in advance, as well as also providing interested persons and other parties with a reasonable opportunity to comment. The "interested persons" component is significant since it allows for inputs from the private sector, civil society, academia and other stakeholders. The USMCA's "good regulatory practices" chapter includes a commitment to undertake regulatory impact assessments in which benefits and feasible alternatives are to be considered.[72]

Applying such an approach to data flows regulation could encourage policy-makers to consider the impact of proposed laws on cross-border data flows as discussed in Chapter 1. It could facilitate domestic debates about the appropriate balance and trade-offs within the context of increasingly digitalized economies and societies. Consideration should also be given to the impact of a restrictive regulation on the quality of a digital product, such as its security features.

Trade negotiations could also commit to publishing domestic regulations affecting data flows, explaining the rationale for the regulation, provide parties with an opportunity to comment and publish reasons for the final approach taken. Inspiration could be drawn from the practice in the WTO Technical Barriers to Trade (TBT) Council, in which members may raise "specific trade concerns", and consider developing a similar process that allows members to discuss regulation in the WTO Council for Trade in Services (CTS) with respect to data flows. Indeed, it is a path already pursued by both the United States and China on existing regulation. Such airing of views is not necessarily binding but it does offer an opportunity for discussion, at a minimum.

International standards

Along the lines of "good regulatory practice", policy-makers worldwide use international standards to align domestic frameworks and, in some cases, reduce trade barriers. Several international standards already exist on the policy issues related to data restrictions – for example, the ISO/International Electrotechnical Commission (IEC) 27000 set of cyber and information security standards; the ISO is also developing standards for privacy. The NIST Framework for Improving Critical Infrastructure Cybersecurity was developed with extensive stakeholder input and helps organizations in the private and public sectors align and prioritize cybersecurity activities, risk tolerance and resources.[73] The NIST Framework references global standards, including ISO and IEC, and may itself become an international standard as it is increasingly adopted globally.[74]

To guide this approach, consideration could be given to developing rules like the WTO TBT Agreement Article 2.4, whereby WTO members agree to use international standards where available as a basis for domestic technical regulation. The presumption is then that the technical regulation is not an unnecessary barrier to trade.[75]

Other standards relevant for data flow concerns, such as those relating to privacy, have been developed in intergovernmental forums among a subgroup of WTO members, for example, in the OECD (OECD Privacy Guidelines) and in the APEC (APEC Privacy Framework). In addition, relevant standards are being developed in internet governance bodies such as the IETF. However, the latter would not qualify as international standards under the WTO TBT Agreement, since they do not meet the requirements of openness because membership of both OECD and APEC is limited.[76] A negotiating party could still commit to considering whether these standards are a suitable basis for domestic regulation and to providing reasons for departing from such standards.

Several PTAs directly refer to standards and interoperability mechanisms. For example, in USMCA, the parties agree that they "should take into account principles and guidelines of relevant bodies, such as the APEC Privacy Framework and the OECD Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data (2013)".[77] Stakeholders consulted for this paper indicated that reference to specific standards within the context of a trade agreement can help provide certainty on the policy landscape and means of compliance. Negotiators could also consider committing to further develop standards in vital areas affected by global data flows where they are not yet available in the relevant standard-setting forums for those issues.

Policy interoperability

Using trade agreements to link domestic regulation to international standards developed in non-trade forums can help reduce regulatory diversity but it is unlikely to produce harmonized outcomes. In areas such as privacy and consumer protection – and also with newly arising regulatory issues set to affect data flows, such as the delivery of online health services – countries' regulatory approaches are grounded in cultural, legal and historical contexts that limit opportunities to harmonize. Even though the OECD and APEC have developed guidance on privacy, these are expressed as principles. Variations exist in the specific manifestation of privacy rules and regulations on personal data flows between OECD and APEC members respectively, with different compliance obligations.

As a result, countries may want to develop mechanisms for linking domestic regulatory systems, helping those companies that move data cross-border comply with standards in multiple jurisdictions. The EU-US Privacy Shield and APEC Cross-Border Privacy Rules are two variations of such international mechanisms (see Figure 6).

Other countries or regions are developing transfer mechanisms to suit their needs. For instance, and as briefly mentioned in Chapter 1, the ASEAN's recently adopted Framework on Digital Data Governance includes a mandate to develop a regional data transfer mechanism for facilitating compliance with data rules the bloc. The recent meeting of ASEAN telecoms and IT ministers approved the approach for developing the mechanism, to include a certification mark for entity compliance and model contractual clauses.[78] ASEAN work is also ongoing on a data classification work stream to clarify policy-makers' data access-related requests.

Figure 6: Illustration of data transfer mechanisms

APEC Cross-Border Privacy Rules (CBPRs)

The APEC Cross-Border Privacy Rules (CBPRs) facilitate the transfer of personal information among APEC members. The CBPR requires businesses to develop privacy policies based on the APEC Privacy Framework (which is based on the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, updated in 2013). The APEC CBPRs are based on the accountability of participants to protect personal data consistently with the APEC privacy principles.[79] APEC accountability agents assess the consistency of businesses' privacy policy and practice with the APEC CBPR requirements. APEC accountability agents and privacy-enforcement authorities are, therefore, responsible for enforcing compliance.[80] According to some stakeholders, however, too few accountability agents mean that the system is expensive and difficult for small businesses to work with.

EU-US Privacy Shield

The Privacy Shield (which replaced the EU-US Safe Harbour framework) allows for flows of personal data between the US and the EU. The EU has certified the Privacy Shield as "adequate" under GDPR, thereby allowing transfers of personal data from the EU to the US by companies participating in the Privacy Shield. Under the Privacy Shield, US companies, through an industry body or individually, self-certify to the US Department of Commerce that they will protect personal data in a manner consistent with the Privacy Framework, which includes the Privacy Shield Principles.[81] Oversight and enforcement is the responsibility of the US Federal Trade Commission and Department of Commerce. An ombudsperson can respond to complaints by EU citizens about access by US intelligence agencies to EU citizens' personal data.

Adequacy, mutual recognition and equivalence

One approach to enabling transfers of personal data is the EU GDPR requirement that the data destination country's privacy protection is "adequate" – understood as being equivalent to GDPR standards. Once this is determined, companies may transfer EU resident data to that jurisdiction. Currently, Argentina, Canada, Israel, New Zealand, Switzerland and Japan are certified as "adequate" by the EU. This in effect leads to regulatory alignment of standards (albeit by means of the data destination country coming into line with the EU GDPR), which is like the so-called "enhanced MRAs" within the EU and in the Australia-New Zealand Closer Economic Relations Trade Arrangement. Alternatively, where there are international standards or principles, governments could aim to develop additional commitments for implementation domestically, while each retains the right to unilaterally determine conformity by data destination countries.[82]

There are other models of MRA and recognition of equivalence that are less ambitious but nevertheless enable interoperability among different regulatory systems. One approach is not to require alignment of the underlying regulation; instead, the regulatory oversight or implementation is done by a counterpart in another jurisdiction, which is recognized as sufficient for the purpose at hand. This can happen when a data destination country (or firms within that country) agree to apply the regulations set by the data source's jurisdiction, which is effectively what occurs for US businesses receiving EU personal data under the EU–US Privacy Shield Agreement. Such arrangements presume that the data destination country has the capacity to enforce compliance with the data source country regulations.

The GATS and WTO TBT Agreement do offer guidance for use of MRAs. While recognition could go a long way in facilitating trade, there is always the risk of exclusion of third parties that do not participate in such arrangements. Article VII of GATS aims to strike a balance between these two aspects. As described earlier in this chapter, this provision requires that there must be one set of substantive criteria according to which recognition is granted. The TBT Agreement also incorporates commitments on MRAs, including clauses ensuring that assessment of conformity with domestic regulation is open, transparent and non-discriminatory.

In practice, most MRAs are linked with PTAs, confirming the preference for bilateral arrangements on areas of potential regulatory sensitivity. Even then, MRAs are difficult to negotiate. Trade policy-makers could therefore consider a multipronged approach to encouraging regulatory cooperation, activating different tools from principles to interoperability to adequacy based on the negotiating parties involved, but consistently aiming for transparent, non-arbitrary and coherent approaches that are implementable by users.

In a multilateral or plurilateral setting, technical assistance could be crafted to support those with a longer way to go on bringing domestic frameworks up to speed, and for the capacity to enter into MRA-like arrangements. Doing so could help bring about a higher level of trustworthiness to the global digital economy, since ensuring compliance with data transfer provisions currently remains one of the biggest challenges.

At a bilateral level, additional efforts might include agreeing that interoperability can be achieved using the law, regulation, voluntary or industry-led regulation, codes of conduct, guidelines and enforcement mechanisms. Countries could also reference specific sectoral arrangements or commit to fleshing out cooperation among domestic policy-makers on issues such as privacy, consumer protection and cybersecurity. Interoperability mechanisms should be the end goal of these sectoral approaches. Greater or lesser detail could be included, depending on the regulatory issue. On cybersecurity, for instance, parties could agree to cooperate and develop best practices concerning risk management.

Conclusion

Finding a balance between permitting the flow of data across jurisdictions and achieving domestic policy objectives such as privacy and security will continue to be a challenge. Yet, for the global economy to function efficiently, efforts to address this challenge must be pursued.

The case for doing so is outlined in Chapter 1. Data flow restrictions are unlikely to lead to long-term benefits globally. Some specific counterexamples may exist, but even these do not fully reflect the complexity of the restrictions' current and potential future impacts, including reduced economic growth, limited imports and exports of services, hampered cybersecurity, reduced financial system oversight, missed scientific advances and less effective environmental intervention.

For instance, local data storage and processing requirements can increase the risk of cyberattacks, while accountability-based data transfer mechanisms, such as the APEC CBPR, demonstrate how data flows and high standards for protecting privacy can coexist. More work may be needed to ensure CBPR-type mechanisms are usable by small businesses that are increasingly operating across borders thanks to technology, as well as entrepreneurs in developing countries.

Trade policy can play a critical role in helping achieve the required balance between data transfer and other policy objectives. Chapter 2 demonstrates that such policy falls into three categories: obligations and disciplines, exceptions, and provisions on regulatory cooperation.

As a starting point, the WTO already contains a range of rules that could support cross-border data flows. Recent PTAs included updated commitments on data flows and agreements to avoid data localization requirements, subject to appropriate exceptions. While these new rules are important, more is required in order to address growing data flow restrictions. Indeed, despite these updated commitments, many of these data flow restrictions may be justified under relevant WTO/PTA exception provisions. Exceptions risk becoming the rule without the further development of mechanisms to bridge regulatory differences between countries.

The third policy category – regulatory cooperation – is needed to raise the level of trust between policy-makers. Typically, trade disciplines have been used to ensure a balance between achieving regulatory objectives and enabling economic liberalization. This paper outlines the domestic steps and corresponding trade rules that can support interoperability and create pathways for data to flow by:

– *Ensuring the least trade restrictive* of available regulatory measures are used to achieve a legitimate policy objective while not intruding on regulatory sovereignty. For data flows this would mean that, while a regulator has the authority to determine the desirable level of protection of a given objective, a trade discipline could require that the regulator uses the least trade-restrictive means to achieve the desired result. Internationally agreed technical standards would help establish a benchmark of what constitutes a least trade-restrictive approach to regulation, similar to the WTO TBT Agreement and its Agreement on the Application of Sanitary and Phytosanitary Measures (SPS). Currently, however, such international standards are not readily available for a range of issues relating to data flows.

– *Calling for sound domestic regulatory principles* such as transparency, simplified procedures, public consultation, advance notice on implementation of changes, establishment of independent regulators, clarity on the sanctions and due process. For data flows, this could start, for example, with the introduction of privacy protection or online consumer protection laws tailored to the digital economy. While trade rules sometimes call for the establishment of regulatory frameworks, they do not set any substantive standards for their content.

– *Encouraging regulatory* cooperation to facilitate cross-border trade. For data flows, this may involve developing international standards. However, even where international standards have been agreed, domestic implementation has been sufficiently varied so that interoperability mechanisms remain necessary, such as recognition of domestic regulatory standards as well as cooperation between regulatory authorities.

– *Requiring that interoperability mechanisms for data flows* reduce the risk of discrimination and the exclusion of third parties. Data transfer mechanisms, mutual recognition or adequacy arrangements between a subgroup of WTO members will result in differentiated treatment of data flows. It will be important, therefore, to ensure that such different arrangements are open to participation by all countries according to a clear set of objective standards.

While trade policy has its limitations and cannot resolve all issues related to data flows, it can play a crucial complementary role in facilitating interactions between domestic regimes. This paper has also noted the desirability of arriving at internationally agreed principles and guidelines for regulatory good practices on "non-trade" objectives. Doing this would almost certainly help to clarify the bounds of what merits justification under an exception to a trade commitment as against what is more likely arbitrary, discriminatory or protectionist responses.

The data flow landscape, both in practice and in the law, will remain an area of critical importance. There is a need to bring different stakeholders from various fields together in a common direction on data flow policy. Leadership on this agenda is an urgent necessity.

Contributors

Authors

Abdelhamid Mamdouh, Senior Counsel, King & Spalding, Switzerland
Anupam Chander, Professor of Law, Georgetown University, United States
Joshua P. Meltzer, Senior Fellow, Global Economy, Brookings Institution, United States
Martina F. Ferracane, Research Associate, European Centre for International Political Economy, Belgium

World Economic Forum

Platform for Shaping the Future of Trade and Global Economic Interdependence

Kimberley Botwright, Community Lead, International Trade and Investment, Switzerland
Nivedita Sen, Intern, Digital Trade, Tax and Competition, Switzerland
Richard Samans, Managing Director, United States
Sean Doherty, Head, International Trade and Investment, Switzerland

Reviewers

Adam Schlosser, Director, International Public Policy, Workday
Andrew Mitchell, Director of Studies, International Economic Law, Melbourne Law School, University of Melbourne
Barbara Kotschwar, Senior Director, Global Government Relations, Visa
Carl Gahnberg, Policy Adviser, Internet Society
François Martins, Head of Government Relations, Brazil, MercadoLibre
Fukunari Kimura, Professor, Faculty of Economics, Keio University
Henry S. Gao, Associate Professor, Singapore Management University, School of Law
Jake Colvin, Vice-President, Global Trade Issues, National Foreign Trade Council
Javier Lopez Gonzalez, Senior Trade Policy Analyst, Organisation for Economic Co-operation and Development
Jennifer Daskal, Senior Associate, Technology Policy Program, Center for Strategic & International Studies
Kimberley Claman, Director, International Government Affairs, Citi
Lisa Pearlman, Head of Global Trade and International Policy, Apple
Magnus Rentzhog, Senior Adviser, Swedish National Board of Trade
Mark Wu, Stimson Professor of Law, Harvard Law School
Martin Molinuevo, Senior Counsel, World Bank Group
Michitaka Nakatomi, Special Adviser, Japan External Trade Organization (JETRO)
Mira Burri, Senior Lecturer, University of Lucerne
Mona Farid Badran, Associate Professor, Cairo University
Nicholas Bramble, Public Policy Manager, Google
Pablo Segura, Data Privacy Senior Manager, Brazil, MercadoLibre
Shin-yi Peng, Professor of Law, National Tsing Huai University
Simon Lacey, Vice-President Global Government Affairs Trade Facilitation and Market Access, Huawei
Steve Stewart, Director, International Trade Policy, IBM
Usman Ahmed, Head of Global Public Policy, PayPal
Wang Huiyao, President, Center for China and Globalization
Weiwei Zhang, International Trade Analyst, Sidley Austin; Adjunct Professor, University of International Business and Economics (UIBE) Law School

Endnotes

1. G20 Ministerial Statement on Trade and Digital Economy, https://www.g20.org/pdf/documents/en/Ministerial_Statement_on_Trade_and_Digital_Economy.pdf.
2. Osaka Declaration on Digital Economy, https://www.g20.org/pdf/special_event/en/special_event_01.pdf.
3. Ferracane, M. F. (2017), *Restrictions on Cross-Border Data Flows: A Taxonomy*, Working Paper No. 1/2017, European Centre for International Political Economy (ECIPE), Brussels.
4. Ibid., Figure 1 at 2.
5. Casalini, F. and J. Lopez Gonzalez (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers, No. 220*, OECD Publishing, Paris, p. 15.
6. The Data Restrictiveness Index varies between 0 (completely open) and 1 (virtually restricted) with higher levels indicating increasing levels of data restrictiveness. Between 2006 and 2017, the index doubled from 0.23 to 0.45. The index covers 64 countries around the world, representing more than 95% of value-added content of gross exports. Ferracane M. F., J. Keren and E. van der Marel (2018), "The Cost of Data Protectionism", *Vox EU*, 25 October 2019, https://voxeu.org/article/cost-data-protectionism.
7. See, for example, Ferracane (2017); Casalini and Lopez Gonzalez (2019).
8. See, for example, Mandel, M. (2013), "Data, Trade and Growth", *Progressive Policy Institute Policy Brief*, 24 April 2013; and Castro, D., and A. McQuinn (2009), "Cross-Border Data Flows Enable Growth in All Industries", Information Technology and Innovation Foundation (ITIF), February 2009.
9. Bauer, M., H. Lee-Makiyama, E. van der Marel and B. Verschelde (2016b), "A Methodology to Estimate the Costs of Data Regulation", *International Economics*, vol. 146, issue 2, pp. 12–39.
10. Leviathan Security Group (2015), *Quantifying the Cost of Forced Localization*, 2015, https://static1.squarespace.com/static/556340ece4b0869396f21099/t/559dad76e4b0899d97726a8b/1436396918881/Quantifying+the+Cost+of+Forced+Localization.pdf.
11. Badran, M. F. (2018), "Economic Impact of Data Localization in Five Selected African Countries", *Digital Policy, Regulation and Governance*, vol. 20, issue 4, pp. 337–357.
12. National Association of Software and Services Companies (NASSCOM)–Data Security Council of India (DSCI) (2013), *Survey of the Impact of EU Privacy Regulation on India's Services Exporters*.
13. Chander, A., and U. P. Lê (2015), "Data Nationalism", *Emory Law Journal*, vol. 64, pp. 677–739.
14. Cory, N. (2017), *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*, Innovation Technology Innovation Foundation (ITIF), 1 May 2017; Blodget, H. (2011), "The Country's Problem in a Nutshell: Apple's Huge New Data Center in North Carolina Created Only 50 Jobs", *Business Insider*, 28 November 2011, https://www.businessinsider.com/apple-new-data-center-north-carolina-created-50-jobs-2011-11?r=US&IR=T; Rosenwald, M. S. (2011), "Cloud Centers Bring High-Tech Flash But Not Many Jobs to Beaten-Down Towns", *The Washington Post*, 24 November 2011, http://www.washingtonpost.com/business/economy/cloud-centersbring-high-tech-flash-butnotmanyjobs-to-beaten-down-towns/2011/11/08/gIQAccTQtN_story.html.
15. Amoroso, E. (2013), "The New Security Architecture", *Dark Reading*, 20 November 2013, www.darkreading.com/compliance/the-new-security-architecture-/d/d-id/899845.
16. See Hutchins, E., M. J. Cloppert and R. M. Amin (2011), *Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains*, Lochheed Martin, https://www.lockheedmartin.com/content/dam/lockheed-martin/rms/documents/cyber/LM-White-Paper-Intel-Driven-Defense.pdf.
17. The list is based on a broader analysis presented in New York Cyber Task Force (2017), *Building a Defensible Cyberspace*, School of International Public Affairs (SIPA), Columbia University, 18 September 2017, https://sipa.columbia.edu/sites/default/files/3668_SIPA%20Defensible%20Cyberspace-WEB.PDF.
18. For a broader analysis on cross-border data flows and security, see Ferracane, M. F. (2019), "Data Flows & National Security: A Conceptual Framework to Assess Restrictions on Data Flows under GATS Security Exception", *Digital Policy, Regulation, and Governance*, Emerald.

19. Global Financial Markets Association (GFMA) (2019), *International Principles to Improve Data Security and Mobility to Support Global Growth*, https://www.gfma.org/wp-content/uploads/2019/05/international-principles-to-improve-data-mobility-privacy-and-security-website-final.pdf. The GFMA also puts forward for consideration principles that could simultaneously balance improving customer data protection, financial system stability and movement of information across borders.
20. Data flow restrictions may complicate regulatory compliance. Different privacy laws and other regulations related to data flows can result in conflicts of law for companies subject to multiple data regimes.
21. Financial Services Board (FSB) (June 2019), *FSB Report on Market Fragmentation*. https://www.fsb.org/wp-content/uploads/P040619-2.pdf.
22. World Economic Forum (September 2018), *The Appropriate Use of Customer Data in Financial Services: Trade-offs and Policy Considerations*.
23. Privacy by design is different from privacy-enhancing technologies in that the former is a requirement at the core of the architecture of a system or product, while the latter are employed at a second stage to strengthen the system after the architecture has already been implemented. See Rachovitsa, A. (2016), "Engineering and Lawyering Privacy by Design: Understanding Online Privacy Both as a Technical and an International Human Rights Issue", *International Journal of Law and Information Technology*, vol. 24, no. 4, pp. 374–399.
24. For an appraisal of US electronic surveillance activities described by Edward Snowden, see Privacy and Civil Liberties Oversight Board (2014), *Report on the Surveillance Program Operated Pursuant to Section 702 of the Foreign Intelligence Surveillance Act*, 2 July 2014, https://www.pclob.gov/library/702-Report.pdf. The revelations raised concerns about foreign government access to personal data and the role of private companies in facilitating these activities. In addition, they led to the invalidation of the Safe Harbor agreement that enabled transfers of personal data from the EU to the US, leading to a new cross-border transfer agreement in the form of the EU-US Privacy Shield. Case C-362/14, Maximillian Schrems v Data Protection Commissioner, Judgement of the Court (Grand Chamber) of 6 October 2015.
25. Rachovitsa (2016), p. 382.
26. Note this categorization is a simplification based on the authors' interpretation in order to provide practical examples for the previous taxonomy.
27. Cooper, G. and H. Le (2018), "Vietnam's New Cybersecurity Law: A Headache in the Making?", *Cyber Security Practitioner*, July, https://www.duanemorris.com/articles/static/cooper_le_cybersecurity_practitioner_0718.pdf.
28. Federal Law No. 242-FZ, "Data Localization Law". An online content law also requires data localization, but for communications information: Federal Law No. 97-FZ, "Online Content Law"; see also Yarovaya Law, Federal Law Nos. 374-FZ and 375-FZ. Mihaylova, I. (2016), "Could the Recently Enacted Data Localization Requirements in Russia Backfire?", *Journal of World Trade*, vol. 50, no. 2, pp. 313–334.
29. Federal Law No. 152-FZ "On Personal Data" of 2006. Russia identifies the following countries as having adequate protection: Costa Rica, Gabon, Kazakhstan, Mali, Qatar, South Africa, Singapore, Angola, Argentina, Benin, Canada, Cape Verde, Chile, Israel, Malaysia, Mexico, Mongolia, Morocco, New Zealand, Peru, South Korea and Tunisia. https://www.huntonprivacyblog.com/2017/08/16/russian-privacy-regulator-adds-countries-list-nations-sufficient-privacy-protections/.
30. For an example of one approach used by a multinational corporation, see Salesforce's description of its transfer programme: https://www.salesforce.com/content/dam/web/en_us/www/documents/legal/Agreements/EU-Data-Transfer-Mechanisms-FAQ.pdf. See also https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/binding-corporate-rules-bcr_en: "Companies must submit binding corporate rules for approval to the competent data protection authority in the EU." For the currently approved sets of standard contractual clauses, see https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/standard-contractual-clauses-scc_en.
31. Regulation (EU) 2018/1807, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018R1807&from=EN.
32. For a discussion on the separation of personal data from non-personal data, see Casalini and Lopez Gonzalez (2019). The study notes potential differences for different sectors, estimating greater costs for firms operating in textile, apparel, food or motor manufacturing industries.

33. Stored Communications Act, 18 USC § 2702(a)(3). See Mulligan, S. (2018), "Cross-Border Data Sharing Under the CLOUD Act", Congressional Research Service (23 April 2018), https://fas.org/sgp/crs/misc/R45173.pdf; Daskal, J. (2019), "Privacy and Security Across Borders", *Yale Law Journal Forum* (1 April 2019), https://www.yalelawjournal.org/forum/privacy-and-security-across-borders.
34. https://www.consilium.europa.eu/en/policies/data-protection-reform/.
35. https://digital.freshfields.com/post/102fm1y/new-draft-of-the-prc-security-assessment-measures-cross-border-data-transfer-is.
36. Vietnam, Law on Cybersecurity, 18 June 2018, https://data.allens.com.au/pubs/pdf/priv/cupriv22jun18.pdf.
37. Reserve Bank of India, Storage of Payment Systems Data, 6 April 2018, https://www.rbi.org.in/Scripts/NotificationUser.aspx?Id=11244&Mode=0.
38. Sharma, Y. (2019), "All You Need to Know About RBI's Data Localisation Directive", https://blog.idfy.com/all-you-need-to-know-about-rbis-data-localisation-directive-2/.
39. Hunter, M., "Update on Korea's Financial Services in the Cloud", https://www.asiacloudcomputing.org/research/2015-research/fsi2015/29-products/298-fsi2015-update.
40. US Department of Health & Human Services, "Guidance on HIPAA & Cloud Computing", https://www.hhs.gov/hipaa/for-professionals/special-topics/cloud-computing/index.html.
41. Pepper, R., et al. (2016), "Cross-Border Data Flows, Digital Innovation, and Economic Growth", in *The Global Information Technology Report 2016* (World Economic Forum).
42. Ahmed, U. and A. Chander (2015), "Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-Border Data Flows". E15 Initiative. Geneva: International Centre for Trade and Sustainable Development (ICTSD) and World Economic Forum.
43. European Medicines Agency (2017), "Data Anonymisation – A Key Enabler for Clinical Data Sharing", https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf.
44. IAEG-SDGs. "Improving Data Flows and Global Data Reporting for the Sustainable Development Goals", https://unstats.un.org/sdgs/iaeg-sdgs/data-flows/.
45. World Economic Forum (2017), "Harnessing the Fourth Industrial Revolution for Oceans", http://www3.weforum.org/docs/WEF_Harnessing_4IR_Oceans.pdf.
46. Chander, A. (2013), *The Electronic Silk Road: How the Web Binds the World Together in Commerce*, Yale University Press.
47. World Trade Organization (2019), "World Trade Report 2019: The Future of Services Trade", https://www.wto.org/english/res_e/publications_e/wtr19_e.htm.
48. An OECD expert group recommends: "Any restrictions to transborder data flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing": OECD (2013), "Privacy Expert Group Report on the Review of the 1980 OECD Privacy Guidelines", *OECD Digital Economy Papers*, no. 229, http://dx.doi.org/10.1787/5k3xz5zmj2mx-en.
49. National Institute of Standards and Technology, *Cybersecurity Framework*, https://www.nist.gov/cyberframework.
50. The UK data protection regulator recently introduced privacy seals for businesses – essentially a stamp of approval that an organization is meeting the compliance requirements of the UK Data Protection Act. This option for cross-border data transfer facilitates the transfer of data between licensed exporters and importers.
51. Countries looking to achieve adequacy with the EU GDPR should factor in the short-term costs of upgrading local firms' capacity on privacy protection. Specific mechanisms, such as the EU-US Privacy Shield, offer another option. In the latter case, only companies that want to process data from that specific country have to comply with all requirements; Mattoo, A. and Meltzer, J. P. (2018), "Data Flows and Privacy: The Conflict and Its Resolution", *Journal of International Economic Law*, vol. 21, issue 4, pp. 769–789.
52. The General Agreement on Trade in Services requires governments to administer services regulations in a "reasonable, objective and impartial manner". See Peng, S. (2019), "The Rule of Law in Times of Technological Uncertainty: Is International Economic Law Ready for Emerging Supervisory Trends?" *Journal of International Economic Law*, vol. 22, issue 1, pp. 1–27.

53. The four modes of supply are: cross-border supply, consumption abroad, supply through commercial presence and supply through the presence of natural persons.
54. Article XXVIII (b) of the GATS.
55. GATS Article XVI:2 (a)–(f).
56. GATS jurisprudence has found that a measure that bans the supply of a service through electronic means, or a subsector thereof, where the service can only be supplied electronically, is equivalent to a zero quota for the service it applies to and, unless listed as a limitation in the schedule, would be inconsistent with market access commitments. (Panel Report, *United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, WT/DS285/R, adopted 20 April 2005, as modified by Appellate Body Report WT/DS285/AB/R, para. 6.285.)
57. GATS Article XVII.
58. Paragraph 5 (c) of the Annex on Telecommunications.
59. The Central Product Classification of the UN.
60. USMCA Article 19.11; CPTPP Article 14.11.
61. Japan-EU FTA Article 8.63.
62. Japan-EU FTA Article 8.65.
63. Japan-EU FTA Article 8.81.
64. CPTPP Financial Services Chapter, Annex 11-B, Section B (Transfer of Information).
65. USMCA Article 17.17.
66. US-Japan Digital Trade Agreement Articles 11–13.
67. Mattoo and Meltzer (2018).
68. OECD (2013), *International Regulatory Co-operation – Addressing Global Challenges*.
69. The following draws from Meltzer, J. P. (2019), "A WTO Reform Agenda: Data Flows and International Regulatory Cooperation", *Brookings Global Economy & Development Working Paper* 130, Global Economy & Development at Brookings, September.
70. WTO, G/TBT/26; USMCA Article 28.2.
71. Basedow, R. and C. Kauffmann (2016), 'International Trade and Good Regulatory Practices: Assessing the Trade Impacts of Regulation", *OECD Regulatory Policy Working Papers* no 4.
72. See USMCA Article 28.11.
73. NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1, April 2018, p. 1
74. Shackelford, S. J., et al. (2015), "Bottoms Up: A Comparison of 'Voluntary' Cybersecurity Frameworks", *University of California Davis Business Law Journal*, vol. 16, p. 217.
75. WTO TBT Article 2.5.
76. Appellate Body Report, EC-Trade Description of Sardines, WT/DS231/AB/R, 23 October 2002, para 227.
77. USMCA Article 19.8.2.
78. Key Approaches for ASEAN Cross Border Data Flows Mechanism, https://asean.org/storage/2012/05/Key-Approaches-for-ASEAN-Cross-Border-Data-Flows-Mechanism.pdf.
79. Asia-Pacific Economic Cooperation (2011), APEC Privacy Recognition for Processors System: Policies, Rules and Guidelines.
80. Asia-Pacific Economic Cooperation (2011), APEC Cross-Border Privacy Rules System: Policies, Rules and Guidelines, 10.
81. Commission Implementing Decision (EU), Adequacy of the Protection Provided by the EU-US Privacy Shield, C/2016/417.
82. Mattoo and Meltzer (2018).

WORLD ECONOMIC FORUM

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