WORLD ECONOMIC FORUM

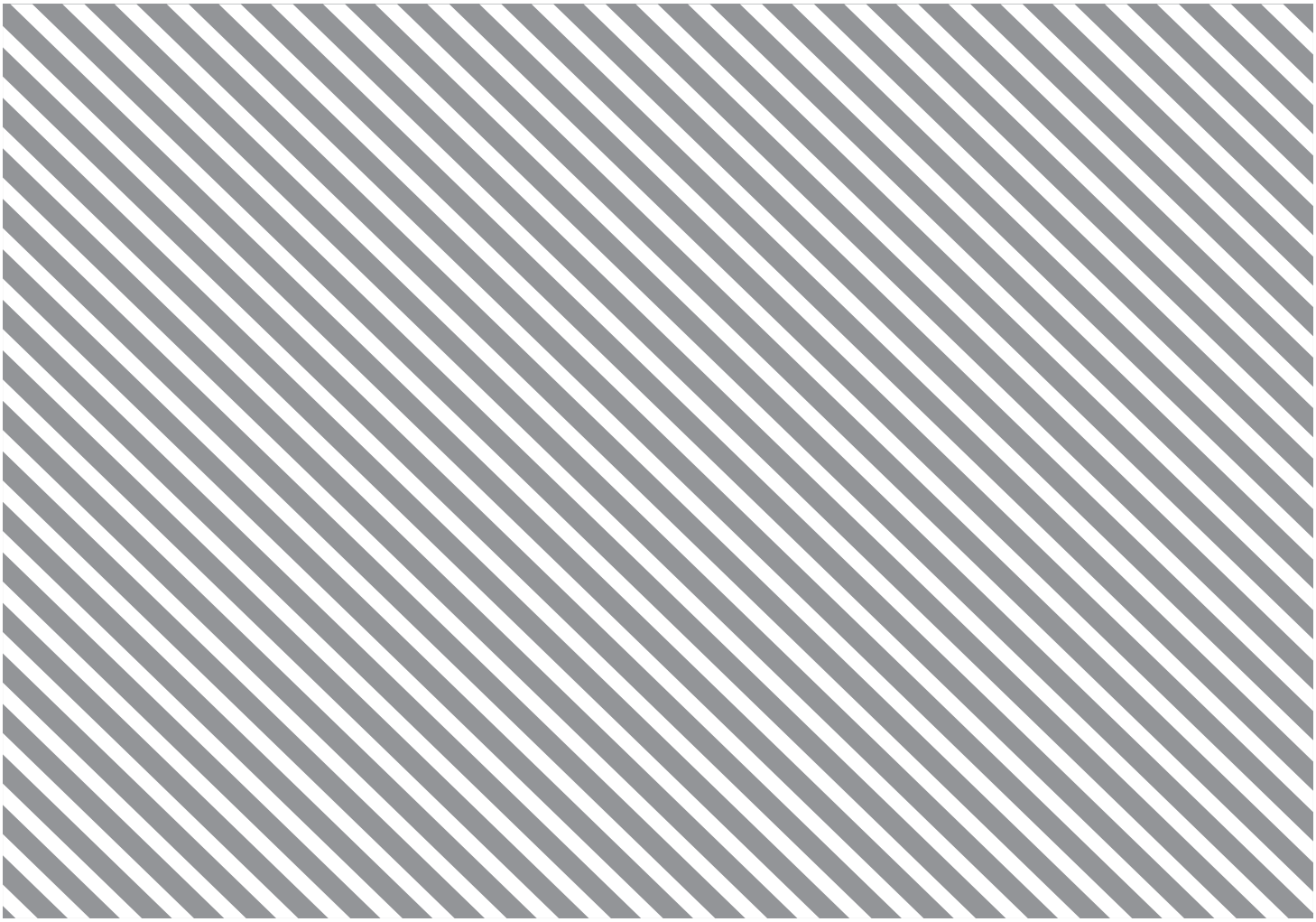
COMMITTED TO IMPROVING THE STATE OF THE WORLD

White Paper

Data Free Flow with Trust (DFFT): Paths towards Free and Trusted Data Flows

Platform for Shaping the Future of Trade and Global Economic Interdependence

May 2020



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

Richard Samans, Managing Director, World Economic Forum

Sean Doherty, Head of International Trade and Investment, World Economic Forum

One of the most critical unsolved challenges of the modern economy is ensuring trust in data flows between countries. In 2020, an estimated 40 zettabytes of data exists in the digital space, which amounts to 40 times more bytes than stars in the universe. Massive volumes of bytes move across borders daily. Data flows are necessary not just for the efficient and smooth functioning of business, but also for consumer-to-consumer interactions. These flows are the backbone of today's diversified value and supply chains. Interconnected infrastructure and services mean that international data flows occur sometimes even for local business operations or consumer communications.

Countries, however, are increasingly fragmented in their approach to data regulation. Data restrictions that prohibit or significantly encumber cross-border data flows have also recently become commonplace in domestic data governance measures. These manifest in different forms and are motivated by a variety of domestic policy objectives, such as privacy, security, access to data and industrial policy. Oftentimes there is an underlying lack of trust, or confidence, that domestic objectives will be achieved if the data moves abroad. Failure to address this lack of trust will see restrictions continue – curbing economic and societal benefits from data flows.

One of the priorities set during Japan's leadership of the G20 in 2019 was the Osaka Track, a term intended to describe efforts needed across various data flow governance processes to meet this challenge. During the World Economic Forum Annual Meeting 2019 in Davos-Klosters, Prime Minister Abe introduced the concept of "data free flow with trust" (DFFT), a vision in which trust and openness in data flows co-exist and complement each other. The term suggests a wider, mutually reinforcing agenda of trade policy, regulatory and business practice cooperation, which together can create the conditions for data to flow across borders at the same time that domestic policy preferences and objectives are satisfied.

Following this important act of leadership, the World Economic Forum Platform for Shaping the Future of Trade and Global Economic Interdependence convened a wide set of stakeholders from industry, international organizations and academia, with diverse geographies represented. Our experts embarked on an intensive process at the beginning of 2020 to map existing policies and frameworks relevant to data flow governance – conceptualized as an "architecture". Discussions during the Annual Meeting 2020 in Davos-Klosters in January and stakeholder meetings in February and March provided the foundations for analysis and the recommendations in this White Paper.

The multidimensional architecture of data flow cooperation outlined in this paper can be read as an initial roadmap for how progress can be advanced practically and holistically on this complex landscape. The paper is intended to inform policy-makers, including those negotiating the Joint Statement Initiative on e-commerce, as well as the private sector. While the latter is not monolithic, there is a potential for it to unite around a core, common set of principles that could enhance the confidence of governments to engage in cooperative solutions that reduce regulatory fragmentation and business uncertainty or transaction costs.

The world has changed significantly since work on this project began. The COVID-19 pandemic is causing unforeseen health and economic crises worldwide. Data flows have been crucial to important aspects of the response, ranging from data sharing for medical research and infection diagnosis to digital services' adoption for business continuity. As interactions have moved online in response to physical distancing restrictions, data flows have spiked, lending added urgency to the need for international collaboration to ensure system-wide confidence, efficiency and safety. This paper provides an initial suggestion of a practical path forward. We commend it to the attention of governments, companies and other stakeholders and look forward to refining these concepts through dialogue on the Forum's platform and beyond.

We would like to express appreciation to rapporteur and principal author Hosuk Lee-Makiyama, Director of the European Centre for International Political Economy (ECIPE). He has done a wonderful job of tying together and framing the many ideas emanating from the consultative process. We also thank the Government of Japan, including the Ministry of Internal Affairs and Communications, the Ministry of Foreign Affairs, and the Ministry of Economy, Trade and Industry, for its vision and practical partnership in this endeavour as well as the project's Steering Committee and core group of eminent scholars and practitioners listed in the Contributors section.

Critical contributions have been made too by the Forum's Governors for the Information and Communication Technologies (ICT) Industry programme associated with the Platform for Shaping the Future of Digital Economy and New Value Creation. Finally, we also thank the project's lead manager, Kimberley Botwright, and our colleagues Nivedita Sen, the project's primary analyst, and Chizuru Suga, Head of the Centre for the Fourth Industrial Revolution Japan, for their invaluable contributions.

The Platform for Shaping the Future of Trade and Global Economic Interdependence provides space for informal, public-private cooperation on key integration policy and practical challenges. Stakeholders work together to shape soft law and other multistakeholder initiatives. Efforts are also under way to improve trade and investment facilitation as well as sustainable value chain operations through best practices and cooperation. Collaboration with governments, business, civil society and academia occurs through dialogue, knowledge sharing and partnerships.

This White Paper is part of a Platform project to help governments develop frameworks for international commerce in increasingly digital-driven economies. The project explores the actions required to ensure that opportunities from emerging technologies enable small and medium enterprises and drive more inclusive trade. It also encourages dialogue on how to navigate the potential disruptive effects of digital trade.

Executive summary

Turning the Data Free Flow with Trust vision into policy action

In his landmark speech at the World Economic Forum Annual Meeting 2019 in Davos-Klosters, Japan's Prime Minister Shinzo Abe invited leaders to build an international order for Data Free Flow with Trust (DFFT). Leaders at the Annual Meeting 2020 provided multistakeholder input to the Osaka Track – a collective term for global governance processes needed to realize the DFFT vision and unleash the benefits from cross-border data flows. The World Economic Forum is heeding the call through dialogue involving leading experts, businesses and stakeholders to turn a landmark speech into a governance architecture.

The world's economies are increasingly data driven as they move towards "Society 5.0". International trade, industrial production and societal functions depend on efficient access to data, while the costs of data restrictions are also increasing. The future of manufacturing with smart and connected industries, as well as the use of data to tackle challenges such as pandemics and ageing societies, highlights the importance of open and trusted data flows for our societies.

The Osaka Track and global data governance do not rely on a single forum for cooperation but depend on international trade, laws and regulation, technology and other areas of governance, involving binding and non-binding rules applicable to governments, businesses or users on multilateral, regional, plurilateral or bilateral levels. This White Paper looks at best practices and examples of international cooperation to achieve open data flows, even in situations where there are few similarities between two legal systems. Nonetheless, a fundamental gap exists on the free flow of non-personal information due to diverging definitions, regulatory approaches (especially on metadata and mixed data sets) and emerging digital protectionism.

Participants in the Forum's dialogue process highlight several recommendations for further advancing the Osaka Track to implement DFFT, including:

- Governments should adopt good privacy and security protections that empower users to individually control rights to their personal information in accordance with international guidelines and standards. Governments should also ensure the availability of multiple mechanisms and derogations for the cross-border transfer of personal data on a non-discriminatory basis for "like" conditions.

- Businesses should support increased consumer trust by proactively establishing it with clients and users by, for example, providing information on data treatment and enhancing transparency.

- Governments should cooperate to develop efficient and innovative mechanisms for issuing and responding to cross-border requests for digital information for law enforcement purposes. Government access to data should also only be pursued where it is legitimate.

- Stakeholders should support and stress the importance of global, market-led, voluntary and consensus-based standards developed by multistakeholder forums involving non-governmental actors, and acknowledge these efforts at intergovernmental forums like those of the Organisation for Economic Co-operation and Development (OECD).

- Interested jurisdictions could initiate public-private dialogue on how to bridge the gaps in definitions and typologies on personal and non-personal data, metadata and sectoral laws.

- Governments should negotiate trade agreements (including at the ongoing Joint Statement Initiative (JSI) negotiations at the World Trade Organization) that include robust obligations in respect of data, while ensuring sufficient discretion to regulate in the public interest, and provisions that facilitate data flows across borders. They should also prohibit requirements to localize the storage and processing of data or to disclose source code, algorithms or encryption keys or other proprietary information relating to cryptography, and prohibit the imposition of tariffs or customs duties on electronic transmissions.

- These commitments should be accompanied by tailored exceptions for legitimate measures that are consistent with existing multilateral rules. All JSI signatories should have multiple transfer mechanisms for personal information reasonably available on a non-discriminatory basis, consistent with the provision of the General Agreement on Trade in Services (GATS), for "like" conditions.

- Many data flow restrictions manifest as forced joint ventures (through foreign equity caps); transfer, and thereby disclosure, of underlying technology, source code, etc.; or a requirement to obtain licences for establishing data centres, undertaking data collection or providing cloud and e-commerce services. More recently, there are plans to restrict the use of algorithms and data applications developed abroad. Market access negotiations should address such disproportionate restrictions.

- Developed economies, international organizations and the business community should provide technical assistance and other capacity-building tools to enable developing economies to pursue high-standard data governance policies and practices.

- Governments and large industry actors should forge public-private partnerships to advise micro, small and medium enterprises (MSMEs) on using digital technologies to drive growth and competitiveness and the ability to reach new markets.

Introduction

DFFT and the Osaka Track

Although the era of digitalization began more than two decades ago, digitalization continues to transform the global economy and societies by bringing markets and people closer to each other. The number of internet-connected devices exceeds the number of people in the world. By 2023, an estimated 29.3 billion networked devices will be in use, with the majority connecting machines, vehicles, infrastructure and buildings rather than users.[1]

The ability to move data globally and securely is of fundamental importance for our society. Yet, domestic rules governing data are increasingly divergent, restrictive and disruptive to global trade and economic and social activities. The absence of effective and trusted policy cooperation mechanisms has turned lawmakers towards other options. Many jurisdictions have introduced discriminatory measures on international data transfers or applied their laws outside their territories. Some studies indicate that the number of data restrictive policies has doubled in the last 10 years.[2]

In his timely message, Japan's Prime Minister Shinzo Abe called for international rules fit for the digital age that carefully protect sensitive data but allow productive data to flow across borders. In his landmark speech at the World Economic Forum Annual Meeting 2019 in Davos-Klosters in January, Prime Minister Abe invited leaders to build an international order for Data Free Flow with Trust[3] – a vision where openness and trust exist in symbiosis, and not as contradictions. In parallel, 76 countries launched new negotiations on digital trade, the so-called ongoing Joint Statement Initiative (JSI) on e-commerce.[4]

Legacy of the 2019 G20 summit and the Osaka Track

In June that same year, trade and digital economy ministers at the G20 Ministerial Meeting in Tsukuba under Japan's chairmanship stressed the significance of cross-border data flows for productivity, innovation and sustainable development,[5] alongside the importance of addressing challenges such as security, data protection and intellectual property that otherwise mar public trust in digital technologies. In other words, "free" flows do not entail a world without appropriate rules or safeguards.

Later at the G20 Osaka Summit, heads of government agreed to work towards the Data Free Flow with Trust (DFFT) vision. The Osaka Leaders' Declaration states that legal frameworks – both domestic and international – should be respected. At the same time, the interoperability between each framework must be enhanced to allow data to flow more freely.[6] The world leaders also confirmed the value of the Osaka Track – a collective term for the global governance processes needed to unleash the benefits of more open and trusted data flows.

The Osaka Track invites discussion on how stakeholders should cooperate across all regions and disciplines to achieve the vision of open and trusted data flows. The World Economic Forum is heeding the call through a dialogue involving leading experts, businesses and stakeholders to turn a landmark speech into an architecture for a more trusted and freer digital economy.

The exercise maps the governance frameworks needed to realize the DFFT vision and the role of business and experts to support greater interoperability for information and knowledge that can be shared in safe and secure ways – through both technical as well as regulatory means.[7] It also highlights the importance of taking a new and innovative approach to data governance in the context of rapid technology transformation as the rigid rules of today will not be able to keep pace.

Towards a data-driven economy

The digital economy (supported by data flows) makes up a sizeable portion of global economic activity. Most attempts to estimate the size of the digital economy conclude that it is equivalent to the size of the gross domestic product (GDP) of a G7 country, and is growing six times faster on average than major emerging markets.[8]

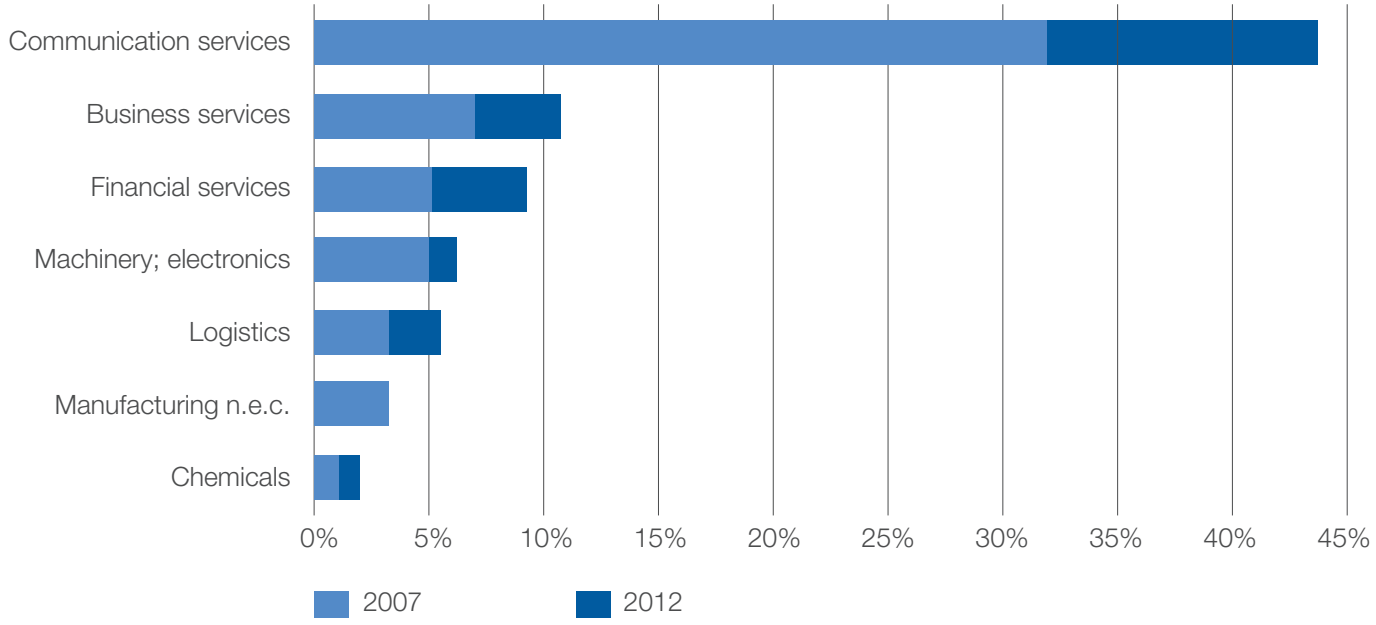
Digitalization has also supported the significant expansion of trade and cross-border business activities, especially in services, where approximately half of cross-border trade is enabled by digital connectivity.[9] In particular, digital trade has allowed developing countries and micro, small and medium-sized enterprises (MSMEs) to export through greater visibility, easier market access and less costly distribution.

Developing countries, for example, accounted for 29.7% of services exports in 2019.[10] Also, with a higher than average share (23%) of women's ownership and management in the tech sector, the digital economy helps women entrepreneurs access global markets.[11]

A more data-intensive economy

Data and connectivity are not just important tools to access overseas markets and customers but are also key ingredients for industrial production. In terms of value, these tools account for between 5% and 45% of all inputs purchased by service or manufacturing businesses in the production process. An effective supply of data, connectivity and software already supersedes the importance of labour and electricity for most industries and is still growing thanks to emerging technologies like machine-to-machine (M2M), next-generation mobile networks (5G), internet of things (IoT) and digital automation. Data flows continue to rely on telecommunications services, and the lack of competition in telecoms markets stifles the flow of data especially for businesses.

Figure 1: Historical increase in data as an input for industrial production, 2007 and 2012 (five-year comparison; selected sectors)



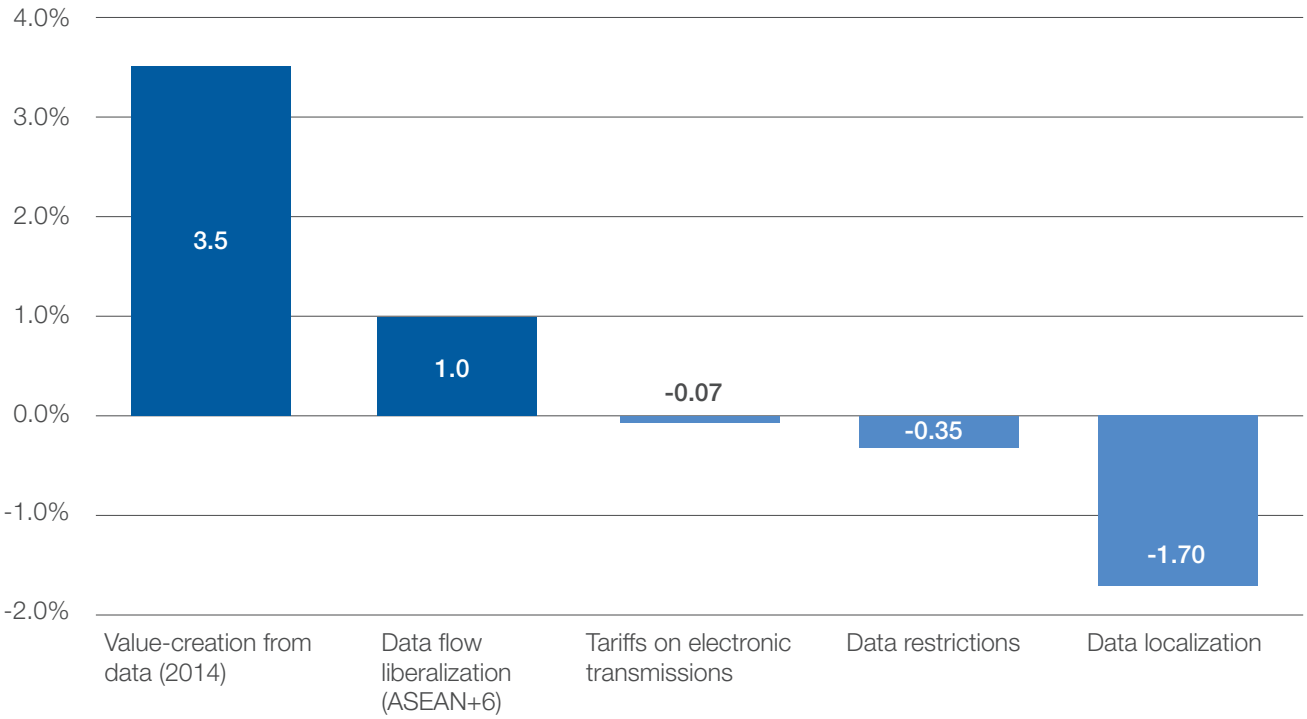
Source: World Economic Forum calculations based on the latest available input-output tables provided by the US Bureau of Economic Analysis (BEA).

The cost of data restrictions

If the efficient use of data and connectivity is a significant productivity-enhancing tool for an economy, restrictions on cross-border data flows are an onerous cost in the international trading system that may change production patterns for many traditional industries. For example, nearly all services sectors (e.g. logistics, retail, professional or financial services) as well as many manufacturing industries (e.g. motor vehicles, machinery, medical and scientific equipment) generate or transmit some form of data, which is routinely stored at one central location globally or regionally.[12]

Regulatory conditions or requirements on transferring data, and data localization policies, i.e. regulatory requirements to store or process data locally, can force exporters to build or lease data centres in every country of operation. Doing so can impose prohibitively high compliance and entry costs. Evidence shows that these requirements also hamper economic growth in the countries that impose them and undo the gains harnessed from digitalization.

Figure 2: Economic impact (GDP) of data flows, cross-border liberalization and restrictive policies



Sources: McKinsey Global Institute, *Digital globalization: The new era of global flows*, 2016, using data provided by Telegraphy; US International Trade Commission, *Digital Trade in the U.S. and Global Economies, Part 2*, 2014; Forthcoming study by S. Evenett and H. Lee-Makiyama; H. Lee-Makiyama, "The Costs of Data Localization", ECIPE, 2014; H. Lee-Makiyama and B. Narayanan, "The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions", ECIPE, 2019.

A few further data points are as follows

- Cross-border data flows added $2.8 trillion (or 3.5%) to world GDP in 2014, surpassing the impact of the global goods trade and 75% of the value accrued to traditional industries.[13] The US International Trade Commission (USITC) estimates the productivity gains from data flows were approximately 3.4-4.5% of GDP in the United States.[14]
- Liberalizing data flows and e-commerce among all members of the Regional Comprehensive Economic Partnership could increase regional GDP by up to 1%.[15]
- Discriminatory tariffs on electronic transmissions generate losses for the local industry and government that are 50 times larger than the claimed tariff revenues.[16]
- Current data flow restrictions and data localization requirements of some countries lower their GDP by up to 0.4% and 1.7%, respectively, depending on the economy and severity of the measure.[17]
- A study conducted on three developing regions (in South America, South-East Asia and Africa) indicates that data localization measures on IoT applications and M2M data could cut 59-68% of their productivity and revenue gains. Such losses of competitiveness also lead to reductions of $4-5 billion in investments and 182,000-372,000 jobs – without any obvious benefits for privacy or local businesses.[18]

Experts universally agree data localization requirements have little positive impact on jobs or security since the productivity losses exceed the minuscule number of jobs created in data processing. Further, experts note that information security is not a function of where data is physically stored or processed geographically but rather how it is maintained.[19] On the contrary, data localization requirements could lower companies' ability to ensure cybersecurity or consumer protection, and could increase entry points for cyberattacks. The Financial Stability Board has also warned that data transfer restrictions could actually limit regulatory oversight.[20]

Case study: Smart and connected industries[21]

The future of industrial production and manufacturing will be at the nexus of wireless connectivity, automation and data-driven applications. As shown in Figure 1, data usage in industrial production is rapidly increasing, with significant impact on how businesses operate and their competitiveness.

The emergence of IoT, where devices, sensors and automated systems communicate with each other, often leveraging on 5G networks (with 20 times shorter latencies and 1,000 times better energy efficiencies than previous networks), will seamlessly connect sensors on industrial equipment, vehicles and infrastructure. In turn, IoT unleashes an unprecedented large-scale collection of data that enables big data analytics and artificial intelligence (AI) to optimize business processes, logistics planning or pricing in real time. Deploying connected devices across the supply chain enables concepts like "smart factories" and digital manufacturing that will radically change the manufacturing locations of the future.

National strategies and visions already exist, such as Germany's "Industrie 4.0" or Japan's "Connected Industries", that connect humans, machines and technologies across borders into systems that continuously create value. For example, the Connected Industries' framework is designed to magnify Japan's national strengths in terms of skills, existing technologies and the *monozukuri* tradition – or its unique understanding of the "factory floor".

Such visions presume that technical infrastructure in different countries can share production data. In this regard, international technical standard-setting bodies play an instrumental role by involving non-governmental actors. Although cooperation has sometimes proved challenging (with some national interests at play), these arrangements are more agile in responding to new technologies than national regulators acting alone.

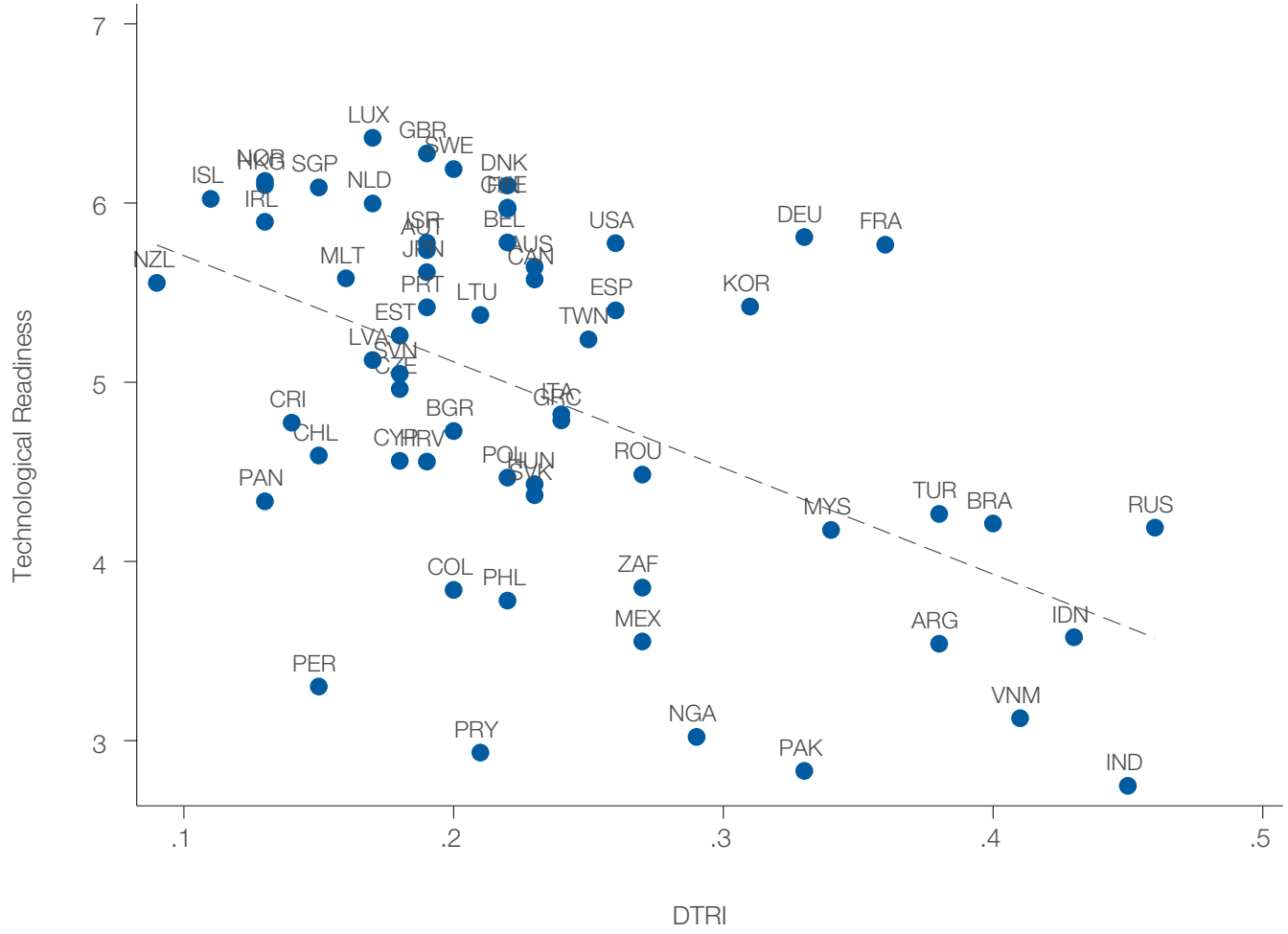
For example, the joint technical committees of the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) develop standards to facilitate technology interoperability, including big data (ISO/IEC 20547), IoT systems (ISO/IEC 21823), machine learning (ISO/IEC CD 23053) and governance implications (ISO/IEC AWI 38507), as well as various standards on trust, risk management and ethics on AI.[22]

National standard-setting bodies are members of ISO and IEC but are often influential on their own, bringing together local and international actors. Entities like the National Institute of Standards and Technology (NIST) in the US, the Japanese Industrial Standards Committee (JISC), the German Institute for Standardization (Deutsches Institut für Normung e.V. – DIN), and the European Committee for Electrotechnical Standardization (CENELEC) and the European Telecommunications Standards Institute (ETSI) within the EU are examples. In addition, there are also sectorial or professional standard-setting bodies relevant for the future of manufacturing, such as the 3rd Generation Partnership Project (3GPP) of primarily network vendors, for mobile network and 5G standards, and the Institute of Electrical and Electronics Engineers (IEEE), with an emphasis on electronics and computing.

Some governments may pursue industrial policies with the objective of creating a local ecosphere (or national "data spaces") or consortiums of data exchanges adhering to their own, unique standards or needs. The promotion of indigenous industries and research, or the notion of *data sovereignty*, sometimes serves as motivation for these initiatives. In time, such policies could impose the *de facto* prohibition of cross-border transfers of data, the use of foreign algorithms or applications, or the mandatory disclosure of source codes.

Current restrictions on foreign ownership in business-to-business industries or intellectual property rights (IPR) issues (like forced transfer of technologies or patent trolling) also impact the uptake of innovative industrial technologies. Research shows how restricting data use is not just an impediment to trade but also to how an economy absorbs new technologies and innovations into its industrial production, which in turn affects its productivity and growth (Figure 3). The negative cost of imposing digital restrictions on industrial data will predictably increase with more data-intensive production methods.

Figure 3: Correlation between countries' ability to adapt new technologies for production (technological readiness) and their digital restrictiveness (Digital Trade Restrictiveness Index)



DTRI - Digital Trade Restrictiveness Index
Sources: World Economic Forum, *The Global Competitiveness Report 2016-2017* (Pillar 9), 2016; M. F. Ferracane, H. Lee-Makiyama and E. van der Marel, *Digital Trade Restrictiveness Index*, ECIPE, 2018.

Broader societal benefits of data

The value of digitalization cannot be captured in purely economic terms. Just as concepts like "Industry 4.0" highlight the digital transformation of manufacturing, "Society 5.0" underscores how digitalization could tackle today's social challenges and usher in broader transformation, rather than just apply within industrial production.

Our societies have evolved from hunter-gatherer (1.0), agrarian (2.0) and industrial (3.0) civilizations to today's information-based (4.0) arrangements. Humankind is now entering into a new "smart" society of sustainable and inclusive socio-economic systems that are powered by big data analytics, AI, IoT and robotics, where digital and physical spaces are tightly integrated.

Data could optimize entire societal and welfare systems – and not just businesses – that tend to people's needs at the time and place required, tailored to the individual to improve their quality of life. For example:

– Data reuse and sharing between government entities as appropriate can tackle ageing society and public health challenges with more accurate preventive care, mitigating increasing costs.

– Data flows can help address pollution, climate change and other sustainability objectives by minimizing waste and increasing traceability across sustainable supply chains.

– Efficient and open access to data are essential for tracking and enabling the delivery of many UN Sustainable Development Goals.

Open access to public data plays a central role in this area. Data collaborations have been set up to facilitate the public-private exchange of information, in addition to data sharing between businesses. Such bottom-up, multi-actor initiatives are key for climate modelling, managing exhaustible resources (e.g. forest and fish stock monitoring), responding to natural disasters and in other areas of public policy or civil contingency planning.[23] These initiatives are not without challenges, however, including those generated by a lack of legal uncertainty created by market regulators, underscoring the importance of improving DFFT governance.

Digitalization has also caused societal challenges that are linked to new technologies and may expose vulnerable groups to new risks. To manage these challenges while delivering benefits, policy-makers must take a human-centric approach to data governance – an approach that is advocated by philosophies like governance innovation.[24] Future policies must be agile and risk- and outcome-based, as domestic regulators and international cooperation will never keep pace with the rate of innovation. New technologies may also achieve better outcomes and compliance than sanctions-based models.

Case study: Data in the service of public health[25]

Countries around the world increasingly face the challenge of delivering affordable healthcare to their citizens. Data-driven technologies are ever more at the centre of healthcare solutions, including aggregating and sharing physiological and medical data, healthcare-site details and infection information.[26]

For example, efficient data collection and open access to data are instrumental for quicker treatment at home, preventive examinations and the early detection of diseases. Personalized healthcare, using AI and other technologies, can promote healthy living and provide optimal and real-time treatment. Online medical solutions empower patients and healthcare professionals by allowing them to monitor conditions, check the progress of treatments and conduct consultations via video connections.

Data innovation is particularly useful to deal with the challenges associated with an ageing society, as low replacement rates are changing the demographic structure of Europe and East Asian countries. The inevitable fact that people live healthier, longer and more productive lives ceases to be a challenge if data-driven cost savings can mitigate the pressure on public finances. One consultancy report predicts that AI applications alone may result in annual savings of $150 billion by 2026 in just the US.[27]

Aggregating genomic, phenotypic and clinical data at a global scale can improve diagnoses and paths to treatment.[28] For example, sharing clinical trial data can lead to new discoveries and strengthen trial results,[29] especially for the development of "orphan drugs" against rare diseases affecting some 10% of the global population that often have genetic causes. Through the World Health Organization (WHO), national governments have stressed the importance of interoperability across national and subnational health data management systems.[30] The WHO advocates global norms for public health emergencies where data sharing should be the default practice, with an onus to explain any reasons for opting out.[31]

However, the sensitivity of healthcare information on multiple levels – for ethical and personal integrity reasons – calls for a degree of care, including the appropriate handling of personal information. As such, most jurisdictions deem healthcare data highly sensitive. Safeguarding trust around health data entails institutional guarantees on privacy protection, duty of care, the management of data accuracy and controlling misinformation. Technical solutions can help deliver these guarantees – through solutions like federated data systems and homomorphic encryption – especially for cross-border purposes.[32]

A best practice for regulating healthcare data is Japan's Next Generation Medical Infrastructure Act, which creates a voluntary nationwide system of anonymized patient treatment and outcome records that is available for trusted and approved medical and healthcare R&D purposes.[33] Similarly, Finland's secondary use of health and social data permits employing healthcare data for purposes other than the primary reason (in accordance with EU General Data Protection Regulation).[34] Leading researchers have also gathered to outline a set of principles for "Authorized Public Purpose Access" that recognizes exceptional conditions during which requirements for consent and anonymization might be waived under emergencies deemed important for public safety or the protection of human life.[35]

Japan's "Security Management Guideline for Cloud Service Providers Handling Medical Information" sets an example for how third parties can certify security requirements.[36] A revised pharmaceutical law (the Pharmaceutical, Medical Devices Act) came into effect in 2014,[37] with the aim to ease the regulatory burden and reduce development costs on software by subjecting them to a less time-consuming certification procedure.

Several countries have recently issued guidelines for health data processing and sharing in the public interest, including data transfers for contact tracing. Key underlying principles include proportionality, least intrusive solutions and application limited to the period of emergency. The COVID-19 pandemic brings into sharp focus the importance and challenges of data sharing in this respect. Swift public health action depends on WHO-coordinated real-time data sharing throughout the outbreak, including the viral genome sequencing and protocols for accurately diagnosing infections, at speeds not seen in previous health emergencies.[38]

The architecture for data governance

The Osaka Track is a process to promote efforts on international rule-making in the area of data flows with trust. Doing so will require global cooperation on international trade, laws, regulation, technology and other areas of governance, as well as rules that are binding and non-binding on governments, businesses and users. To date, governments, industry and user groups have engaged in both intergovernmental and multistakeholder forums to develop international norms, guidelines, principles and standards. Yet, there is no singular forum for all issues relating to global data governance.

These activities can seem to overlap or counteract each other but, by and large, they are complementary, with each forming a pillar of the architecture for global data governance. In each pillar, cooperation takes place on multilateral, regional, plurilateral or bilateral levels where there is sufficient trust and common interests among the parties.

Domestic requirements and international cooperation on cross-border data flows can be categorized into at least four pillars, each with a different and non-mutually exclusive purpose: transfer mechanisms, legal and regulatory cooperation, technical standards and industrial cooperation, and international trade rules.

While some jurisdictions are open and make no distinction between foreign or domestic entities in their data protection rules, most jurisdictions make a distinction between domestic and foreign entities for data that is perceived to pertain to national security, or they designate specific entities as either trusted or of particular high risk – where some jurisdictions also routinely categorize all data as being sensitive.

Figure 4: Osaka Track architecture for data governance

	Relevant pillars for international cooperation on data flows			
	Transfer mechanisms	**Legal and regulatory cooperation**	**Technical standards and industrial cooperation**	**International trade rules**
Universal availability	Unilateral openness (no restrictions imposed) User consent and other legitimate grounds for data transfer (e.g. contractual reasons, public interest) Accountability-based mechanisms (binding corporate rules and standard contract clauses)	Binding international treaties on legal harmonization (Budapest Convention)	Standard-setting in multistakeholder forums (ISO/IEC, IEEE, 3GPP, among others)	World Trade Organization rules (case law, General Agreement on Trade in Services, and Reference Paper and Annex on Telecommunications) with privacy and other exceptions, along with two-tier test (for least-trade restrictiveness and necessity) Ongoing World Trade Organization Joint Statement Initiative negotiations
Limited participation	Adequacy decisions to jurisdictions with adequate protection, e.g. EU-Japan reciprocal adequacy, adequacy decision on the EU-US Privacy Shield Certification programmes (under government oversight), e.g. Asia-Pacific Economic Cooperation Cross-Border Privacy Rules "Trusted" entity schemes	Regional model laws on e-commerce, cross-border data flows and privacy (EU, ASEAN) Principles and guidelines on data flows and privacy (OECD Privacy Guidelines, APEC Privacy Framework) Legal assistance through mutual legal assistance treaties or international conventions Judicial redress and recourse offered to a list of countries under domestic law Diplomatic instruments and strategic partnerships (e.g. Australia-Singapore Digital Economy Agreement)	National and regional standard-setting, e.g. United Nations Economic Commission for Europe Exclusive "data spaces" initiatives and consortium Bilateral mutual recognition agreements or equivalence decisions	Digital trade commitments (e.g. data flow, prohibition on localization and source code access disciplines derived from the Comprehensive and Progressive Agreement for Trans-Pacific Partnership - CPTPP) developed in the Japan-US Digital Trade Agreement, the United States-Mexico-Canada Agreement (USMCA), EU texts, the Digital Economy Partnership Agreement - DEPA, with varying exceptions

Source: World Economic Forum

At the outset, before international cooperation comes into play, domestic policies set conditions or limitations to transfer data – most commonly for privacy objectives. Many countries have designated specific *transfer mechanisms* where personal information may flow overseas under certain conditions or instruments.[39] Notably, many jurisdictions acknowledge user consent, contractual reasons or public and legitimate interests as a derogation to a prohibition to the overseas transfer of personal information. Governments may also pre-authorize binding instruments that provide appropriate safeguards between subsidiaries in a company group, provided that the legal obligations "travel with the data" outside the territory of its origin for either trust or competitive reasons. Some jurisdictions apply such conditions for transfer on a case-by-case basis.

Jurisdictions may decide that a third country guarantees an adequate level of data protection to allow data flows, in so-called adequacy decisions that are increasingly reciprocal.[40] Even between jurisdictions that do not deem each other adequate or equivalent, authorities may still sufficiently trust the private sector in some jurisdictions through certification programmes where companies are liable to provide equivalent protection of the data when it is transferred abroad. Although the certification process may allow for self-certification, relevant government agencies guarantee the enforcement of compliance.

Legal and regulatory cooperation comprises intergovernmental efforts for best practice and common normative principles, and even goes towards the harmonization of domestic laws. Notably, the OECD has developed detailed guidelines on privacy legislation that encourage the harmonization of domestic regulations among its members in this area, which are also referenced in some trade agreements.[41] Regulatory cooperation is also under development within ASEAN, where legal alignment on data governance definitions and privacy is developed concurrently with internal data flow mechanisms.[42]

In the area of law enforcement, the Budapest Convention under the Council of Europe (COE) has 67 signatories, including non-members of the COE from outside Europe. In the first instance, signatories have agreed to designate certain acts as criminal within their legal systems, but some participating signatories also provide each other with legal assistance for offences jointly defined as criminal. Under the same principle of dual criminality, bilateral mutual legal assistance treaties (MLATs) provide legal assistance against illicit activities that originate in another jurisdiction.

Regulatory cooperation converges in some cases with *technical standardization and industrial cooperation* that usually take place in wider and multistakeholder forums. For example, the IEEE or the joint technical committees of the ISO/IEC develop standards and best practices to facilitate technology interoperability, while 3GPP sets the standards for the telecommunication industry.[43] There are also industrial cooperation agreements between governments in the life sciences, electronics and machinery sectors covering technical cooperation, IPRs, research and development, as well as mutual recognition agreements (MRAs) on industrial standards. Other mechanisms include diplomatic instruments and strategic partnerships, such as the recent Digital Economy Agreement between Australia and Singapore,[44] with associated memoranda of understanding on data innovation and AI.

If legal, regulatory and technical cooperation primarily builds trust that enables openness, the role of *trade rules* is to establish binding disciplines to safeguard that openness, where contracting parties of trade agreements commit to not discriminate against each other in agreed areas. At a multilateral level, many World Trade Organization (WTO) rules are relevant to the digital economy, although they may predate the creation of the internet. Also, a WTO panel has taken the view that WTO members are bound to allow information transfers in sectors where they have scheduled market access or national treatment commitments.[45] Invoking privacy exceptions to those commitments would also be subject to conditions.[46]

Services covered by a WTO members' schedule may also benefit from an obligation in the GATS Annex on Telecommunications that grants access to "public telecommunications transport networks" to provide services.[47] Another obligation on data flows is listed in the Understanding on Commitments in Financial Services, where participating members agree not to take any measures that would prevent the transfer of data, with caveats for privacy and confidentiality.[48]

More recent trade rules include the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) concluded in 2017 between 11 countries. The CPTPP contains core commitments that are essential for DFFT, including provisions on the cross-border transfer of information,[49] the prohibition of data localization as a condition for conducting business,[50] limits on the mandatory disclosure of source code (later amended with algorithms),[51] and a ban on the imposition of customs duties on electronic transmissions.[52]

Later trade agreements build on these provisions and their exceptions. Notably, the United States-Mexico-Canada Agreement (USMCA) and the Japan-US Digital Trade Agreement incorporate information transfer for financial services and more specific commitments on algorithms or privacy.[53] The Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore, and recent EU free trade agreement negotiating texts contain a similar scope with different exceptions.

Challenges to cooperation and interoperability

The balance in Prime Minister Abe's speech and the duality of the DFFT – that data flows where there is trust – are critical to the Osaka Track. The notion of interoperability is also central since it can foster trust through all the pillars of the Osaka Track. However, the wider societal challenge does not end there: technical infrastructure is needed to share data and ensure its cross-system usage. Even more broadly, people must be able to make sense of the data and apply it in new contexts.[54]

Openness, trust and interoperability today are conditioned on efficient cooperation where governments, businesses and users can effectively mitigate risks and ensure protection when data is transferred abroad. Such trust is often reciprocal by nature, and arises more readily between entities that are prepared to abide by similar rules or offer equivalent levels of protection against risks. Jurisdictions that share similar legal concepts, and offer effective enforcement and recourse to address any negative externalities arising from data flows between them, are more likely to share trust. Systems with deeper similarities – on constitutional order, ethical values or understanding of fundamental rights – are also less likely to diverge their rules in the future, even as new technologies emerge or regulations are enacted.

Even so, there are examples of international cooperation taking place between countries that are still on a path to develop trust. Given the open nature of the internet and the global trading system, governments must also leave room for alternative mechanisms (like the certification of trusted businesses) when intergovernmental cooperation cannot provide an immediate solution.

Since many trust challenges centre around differences in treatment of personal data, however, some stakeholders have called for a focus on "non-personal data". These voices note that non-personal (and industrial) data is a critical input to the industry and involves less divisive policy issues, making a multilateral consensus more likely. Yet, the cross-border flow of non-personal data still depends on the granular details that govern the local definition of personal data since it is defined negatively, *e contrario*, as any data that is not personal information.

As such, even cross-border flows of non-personal data are subject to complications. Certain jurisdictions determine specific types of *metadata* (i.e. sources of collection, payment data, employee identification or usernames, internet provider addresses, email) or network identifiers like phone numbers and MAC or IP addresses as personal information, while other jurisdictions do not.[55] Similarly, vehicle identification numbers or serial numbers of devices and geospatial information are not directly identifiable, unless the information is combined with other data. As nearly all cross-border data flows contain metadata, some jurisdictions could apply the full scope of their privacy laws although it consists predominantly of non-personal data.[56]

Although many regulations are based on protecting certain data *subjects* – personal data that describes subjects, i.e. users – some regulations restrict data use in sectors that are deemed as sensitive regardless of whether that information is personal or non-personal. For example, some jurisdictions restrict the international transfer of any data that is held by financial institutions, online payment services, trading or business records and healthcare providers.[57]

New legislation may even discriminate against data objects of foreign origin, such as algorithms or applications, from being used in a country without prior authorization. Certain governments grant themselves access to proprietary source codes for software and AI algorithms.[58] There are also examples for *ex ante* licensing requirements for collecting relatively simple data, such as data for autonomous driving or e-commerce activities.

Recommendations to advance the Osaka Track

Discussions with World Economic Forum stakeholders on realizing the DFFT vision identified many forums, pillars and levels of cooperation that shape global rules on data governance. Openness and interoperability for cross-border data flows are conditioned on mechanisms and collaboration that build trust. The architecture for the Osaka Track (Figure 4) illustrates how pathways to free and trusted data flows are possible in various configurations. The architecture can be improved upon, however, and the mapping process revealed crucial gaps.

The Osaka Track needs to fill these gaps in all pillars and levels of cooperation in view of the evidence presented above on the rising incidence of regulatory restrictions, and to address restrictions placed on emerging technologies. Turning off the taps on data flows would reverse the benefits gained from connectivity and digitalization. Failure to ensure continued data flows would result in missed innovations, economic gains and societal advances. Governments will impose irreparable losses on citizen welfare and industrial competitiveness if they adopt disproportionate restrictions.

The development dimension is also important to consider. According to UNCTAD, only around 66% of 107 countries to date have enacted privacy laws or privacy protections and only 56% of 125 countries have online consumer protection laws – with lags in many least-developed countries.[59] In some cases, debates continue regarding new laws; in others, the conversation still centres on achieving connectivity for those not yet online.

The following lays out recommendations to advance various layers of the DFFT architecture. In discussions to prepare this paper, stakeholders largely agreed that a secure and trusted transfer mechanism could be implemented between any two countries at any level of trust, given the widespread use of the safeguard and accountability mechanisms currently available. This offers hope that the Osaka Track can be advanced at a global scale, as well as with variable geometry, in a regional context or among groups of like-minded countries.

On personal information and transfer mechanisms

- Governments should adopt good privacy and security protections that empower users to individually control rights to their personal information in accordance with international guidelines and standards. Stakeholders have particularly noted the importance of the OECD Privacy Framework and the Asia-Pacific Economic Cooperation (APEC) Privacy Framework.

- Businesses should support increased consumer trust by proactively establishing it with clients and users by, for example, providing information on data treatment and enhancing transparency.

- Transfer mechanisms are essential since data otherwise becomes subject to *de facto* localization. This paper outlines several transfer mechanisms that allow a trusted flow of personal information to third countries, even under circumstances where jurisdictions do not offer similar levels of protection. Some rules are applied extraterritorially and "data protection travels with the data". Governments should, therefore, ensure the availability of multiple mechanisms and derogations for the cross-border transfer of personal data on a non-discriminatory basis for "like" conditions.

- Those jurisdictions that apply unilateral or reciprocal adequacy decisions should be encouraged to expedite these decisions and base them on well-defined and transparent criteria according to procedural fairness.

- Certification programmes like the APEC Cross-Border Privacy Rules (CBPR) or the EU-US Privacy Shield are effective for building trust between otherwise non-equivalent systems. However, some stakeholders expressed concerns about the lack of interoperability and openness of these systems, especially for developing countries outside the relevant regional and plurilateral forums. Public-private dialogue among responsible jurisdictions and stakeholders could help alignment and transparency.

On legal and regulatory cooperation

- Governments should recognize the importance of non-personal data and M2M communications to the growth of the global economy and should refrain from restricting their cross-border flow. Many stakeholders agreed that such data, or data that is anonymized, pseudonymized, protected or publicly available, is not personal information.

- A clear area for law enforcement and legislative cooperation is government access to digital information. Governments should cooperate to develop efficient and innovative mechanisms for issuing and responding to cross-border requests for digital information for law enforcement purposes. This includes enhancing the speed and operation of MLATs to make them effective in the digital age, as well as drawing on national or regional legislation to develop approaches to cross-border lawful access requests that are transparent, interoperable and grounded in the rule of law and international human rights principles.

- Since delivering government data access adds costs and can create a conflict of laws, firms and authorities should build consensus on what information is necessary for authorities to do their jobs. Government access to data should also only be pursued where it is legitimate, i.e. the public authority has a legally established capacity and the desired access relates to the function the public authority exercises.

On standardization and technical cooperation

– Stakeholders should support and stress the importance of global, market-led, voluntary and consensus-based standards developed by multistakeholder forums involving non-governmental actors, and acknowledge these efforts at intergovernmental forums like those of the OECD. While governments should participate in such processes, some stakeholders suggest they should refrain from mandating either the procedures by which standards are developed or the substance of those standards, including in instances where the standards may be used as a means of demonstrating compliance with regulatory requirements.

– Interested jurisdictions could initiate public-private dialogue on how to bridge the gaps in definitions and typologies on personal and non-personal data, metadata and sectoral laws. This dialogue should bring together experts from different spheres, including trade policy-makers and data protection regulators, among others. In this context, some stakeholders have even called for a new multistakeholder forum for M2M and industrial data sharing to support existing technical and regulatory processes. Others have suggested setting up MRAs for industrial data standards.

– Beyond targeted government-to-government engagement, policy-makers should ensure that domestic measures affecting data are enacted in a transparent manner that allows opportunities for broad stakeholder input; are evidence-based and consider the technical and economic feasibility of requirements; require the publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted and proportionate, and restrict trade as little as possible. Some stakeholders also stress the importance of enabling reliance on global standards in satisfying regulatory or certification requirements.

On international trade negotiations

– Governments should negotiate trade agreements (including at the ongoing JSI negotiations at the WTO) that include robust obligations in respect of data, while ensuring sufficient discretion to regulate in the public interest. Complementary obligations on online consumer protection and personal information could improve systemic confidence in the digital economy and trust between different parties.

– Specifically, many recent trade agreements (such as the CPTPP, USMCA, Japan-US Digital Trade Agreement) already include provisions that facilitate data flows across borders; prohibit requirements to localize the storage and processing of data or to disclose source code, algorithms or encryption keys or other proprietary information relating to cryptography; and prohibit the imposition of tariffs or customs duties on electronic transmissions. Bilateral, plurilateral and regional trade agreements should include further commitments on new digital technologies, including AI, FinTech and electronic payments.

– These commitments should be accompanied by tailored exceptions for legitimate measures that are consistent with existing multilateral rules. All JSI signatories should have multiple transfer mechanisms for personal information reasonably available on a GATS-consistent, non-discriminatory basis for “like” conditions.

– Some stakeholders note how telecommunications providers face challenges in ensuring data flows in closed or inadequately regulated markets. Both preferential and multilateral commitments (that are often based on the original WTO Reference Paper on basic telecommunications) should be updated to reflect the internet age, including non-discrimination for wholesale access, licensing and market access for business markets.

– Many data flow restrictions manifest as forced joint ventures (through foreign equity caps); transfer, and thereby disclosure, of underlying technology, source code, etc.; or a requirement to obtain licences for establishing data centres, undertaking data collection or providing cloud and e-commerce services. More recently, there are plans to restrict the use of algorithms and data applications developed abroad. Market access negotiations should address such disproportionate restrictions.

On what governments can do for development

– Developed economies, international organizations and the business community should provide technical assistance and other capacity-building tools to enable developing economies to pursue high-standard data governance policies and practices to further enhance their success at bringing the benefits of digitalization to their citizens. This is critical since data governance gaps add challenges and limit available policy options, particularly if advanced economies do not trust the standard of treatment of data in the developing economies. Transfer mechanisms should be designed so compliance costs and complexity do not hinder developing countries and MSMEs from participating in global trade.

– Governments and large industry actors should forge public-private partnerships to advise MSMEs on using digital technologies to drive growth and to reach new markets.

Contributors

Steering Committee

Nobuhiro Endo, Chairman of the Board, NEC Corporation, Japan

Anabel Gonzalez, Non-Resident Senior Fellow, Peterson Institute for International Economics, USA

Merit Janow, Dean, School of International Public Affairs, Columbia University, USA

Paul Thomas Jenkins, Chair of the Board, OpenText Corporation, Canada

Hiroaki Nakanishi, Executive Chairman, Hitachi, Japan

Ngozi Okonjo-Iweala, Chair, Gavi, the Vaccine Alliance, USA

Richard Samans, Managing Director, World Economic Forum

Takahito Tokita, President and Representative Director, Fujitsu, Japan

Experts Committee

Usman Ahmed, Head, Global Public Policy, PayPal, USA

Chisato Amano, Expert, ICT and Policy Analysis, Global Public Policy Relations Planning Office, Corporate Strategy Division, NEC, Japan

Jake Colvin, Vice-President, Global Trade and Innovation, National Foreign Trade Council (NFTC), USA

Sadie Creese, Professor of Cybersecurity, University of Oxford, United Kingdom

Haishan Fu, Director, Development Data Group, World Bank, USA

Urs Gasser, Executive Director, Berkman Klein Center for Internet & Society; Professor of Practice, Harvard University, USA

Matthew Gravelle, Director, Group Public and Regulatory Affairs, Compliance, Standard Chartered Bank, United Kingdom

Ichiro Hara, Managing Director, Keidanren (Japan Business Federation), Japan

Brian Hengesbaugh, Chair, Global Data Privacy and Security Business Unit, Baker McKenzie, USA

Austin Imperato, Chief of Staff, Government and Regulatory Affairs, IBM, USA

Josh Kallmer, Executive Vice-President, Global Policy, Information Technology Industry Council (ITI), USA

Barbara Kotschwar, Senior Director, Global Government Engagement, Visa, USA

Tilmann Kupfer, Vice-President, Trade and International Affairs, BT Group, Belgium

Javier Lopez Gonzalez, Senior Trade Policy Analyst, Trade and Agriculture Directorate, Organisation for Economic Co-operation and Development (OECD), Paris

Francois Martins, Head, Government Relations, Brazil, MercadoLibre, Argentina

Hiroaki Miyata, Professor and Chair, Department of Health Policy Management, Faculty of Medicine, Keio University, Japan

Martin Molinuevo, Senior Counsel, World Bank Group, Washington DC

Michitaka Nakatomi, Special Adviser, Japan External Trade Organization (JETRO), Singapore

Jun Nakaya, Manager, Global Relations, Public Policy and Business Development Office, Fujitsu, Japan; Chair, Trade Policy Committee, Japan Electronics and Information Technology Industries Association (JEITA), Japan

Annabella Ng Li Jia, Head, Regional Government Affairs Strategy, Grab, Singapore

Julia Nielson, Deputy Director, Trade and Agriculture Directorate, Organisation for Economic Co-operation and Development (OECD), Paris

Amitendu Palit, Senior Research Fellow, National University of Singapore, Singapore

Lisa Pearlman, Head, Global Trade and International Affairs, Apple, USA

Ulf Pehrsson, Vice-President, Government and Industry Relations, Telefonaktiebolaget LM Ericsson, Sweden

Motohiko Sato, Senior Manager, Policy and Regulatory Analysis Section, Public Policy Office, Rakuten, Japan

Joseph Whitlock, Director, Policy, BSA - The Software Alliance, USA

Satoshi Yoshizawa, Senior Strategist, Technology Strategy Office, Hitachi, Japan

World Economic Forum

Kimberley Botwright, Community Lead, International Trade and Investment

Sean Doherty, Head, International Trade and Investment

Richard Samans, Managing Director

Nivedita Sen, Analyst, Trade and Investment

Rapporteur

Hosuk Lee-Makiyama, Director, European Centre for International Political Economy (ECIPE), Belgium

Endnotes

1. Cisco, “Cisco Annual Internet Report (2018-2023)”, White Paper, 2020.
2. VOX, Centre for Economic Policy Research (CEPR) Policy Portal, “The cost of data protectionism”, 2018; World Economic Forum, “Exploring International Data Flow Governance”, White Paper, 2019.
3. Abe, Shinzo, *Toward a new era of hope driven economy,* 23 January 2019, speech presented at the Word Economic Forum Annual Meeting 2019, Davos-Klosters, https://www.weforum.org/agenda/2019/01/abe-speech-transcript/.
4. World Trade Organization Joint Statement on Electronic Commerce, WT/L/1056, 25 January 2019.
5. Government of Japan, Ministry of Economy, Trade and Industry (METI), “G20 Ministerial Statement on Trade and Digital Economy”, 9 June 2019, https://www.meti.go.jp/press/2019/06/20190610010/20190610010-1.pdf.
6. Government of Japan, Ministry of Foreign Affairs (MOFA), “G20 Osaka Leaders’ Declaration”, 29 June 2019, https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html.
7. Gasser, Urs, “Interoperability in the Digital Ecosystem”, Berkman Klein Center for Internet & Society, Harvard University, Research Publication no. 2015-13, 2015.
8. In the *Digital Economy Report 2019*, the United Nations Conference on Trade and Development (UNCTAD) estimates that up to 15.5% of global GDP is predominantly generated by business-to-business (B2B) digital activities. According to eMarketer in its *Worldwide Retail and Ecommerce Sales* report published in 2018, the turnover of e-commerce transactions alone was $2.7 trillion in 2017 with 25% growth per year. The US Bureau of Economic Analysis estimated the digital economy accounted for 6.9% of US GDP (or $1.35 trillion) in 2017 (Bureau of Economic Analysis, “Digital Economy Accounted for 6.9 Percent of GDP in 2017”, 2019).
9. United Nations Conference on Trade and Development (UNCTAD), “International Trade in ICT Services and ICT-enabled Services”, Technical Note no. 3, 2015; see also Nicholson, Jessica and Ryan Noonan, “Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services”, *Current Politics and Economics of the United States, Canada and Mexico*, vol. 19, no. 1, 2017.
10. United Nations Conference on Trade and Development (UNCTAD), *Handbook of Statistics*, 2019.
11. International Trade Centre (ITC), *Unlocking Markets for Women to Trade*, 2015; ITC*, Digital Economy Unlocks Doors for Women Entrepreneurs in Africa*, 2016.
12. National Board of Trade of Sweden, *No Transfer, No Production*, 2015.
13. McKinsey Global Institute, *Digital globalization: The new era of global flows*, 2016, using data provided by Telegraphy.
14. US International Trade Commission (USITC), *Digital Trade in the U.S. and Global Economies, Part 2*, 2014.
15. Forthcoming study by Simon Evenett and Hosuk Lee-Makiyama, Swiss Institute for International Economics and Applied Economic Research, University of St. Gallen (SIAW), 2020.
16. Lee-Makiyama, Hosuk and Badri Narayanan, “The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions”, ECIPE Policy Brief, 2019.
17. Lee-Makiyama, Hosuk, “The Costs of Data Localization”, European Centre for International Political Economy (ECIPE), 2014; Bauer, Matthias, Hosuk Lee-Makiyama and Erik van der Marel, “Data Localisation in Russia: A Self-imposed Sanction”, European Centre for International Political Economy (ECIPE), 2015.
18. Lee-Makiyama, Hosuk, Badri Narayanan and S. Lacey, “The Impact of Data Localization on IoT – a GSMA study”, GSM Association (GSMA), 2020, forthcoming.
19. World Economic Forum, “Exploring International Data Flow Governance”, White Paper, 2019.
20. Financial Stability Board (FSB), *FSB Report on Market Fragmentation*, 2019.
21. Thanks go to Michitaka Nakatomi, Special Adviser, Japan External Trade Organization (JETRO) and Consulting Fellow, Research Institute of Economy, Trade and Industry (RIETI), and to Urs Gasser, Executive Director, Berkman Klein Center for Internet & Society, and Professor of Practice, Harvard University, for their valuable input.

22. The ISO/IEC JTC 1/SC 42 international standards committee is currently developing various AI-related standards, such as a framework for AI systems using machine learning, risk management, an overview of trustworthiness, and governance implications of the use of AI by organizations (see "Standards by ISO/IEC JTC 1/SC 42 – Artificial intelligence" at https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0).

23. GovLab, "Data Collaboratives Explorer", https://datacollaboratives.org/explorer.html.

24. Study Group on a New Governance Model in Society 5.0, *Governance Innovation: Redesigning Law and Architecture in the Age of Society 5.0*, 2020, https://www.meti.go.jp/english/press/2019/pdf/191226001.pdf.

25. Thanks go to Hiroaki Miyata, Professor and Chair, Department of Health Policy Management, Faculty of Medicine, Keio University, Japan, for his valuable input to this section.

26. Government of Japan, Cabinet Office, "Examples of Creating New Value in the Fields of Healthcare and Caregiving (Society 5.0)", https://www8.cao.go.jp/cstp/english/society5_0/medical_e.html.

27. Forbes, "AI and Healthcare: A Giant Opportunity", 11 February 2019.

28. World Economic Forum, "Global Data Access for Solving Rare Disease: A Health Economics Value Framework", White Paper, 2020.

29. European Medicines Agency, *Data anonymisation – a key enabler for clinical data sharing*, 30 November – 1 December 2017 Workshop report, 2018, https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf.

30. World Health Organization, *WHO guideline: Recommendations on Digital Interventions for Health System Strengthening*, 2019, https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1.

31. Modjarrad, Kayvon, et al., "Developing Global Norms for Sharing Data and Results during Public Health Emergencies", *PLoS Medicine*, vol. 13, no. 1: e1001935, 2016.

32. World Economic Forum, "Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data", White Paper, 2019.

33. Government of Japan, "Act Regarding Anonymized Medical Data to Contribute to R&D in the Medical Field" ("Next Generation Medical Infrastructure Act", 28 April 2017).

34. Government of Finland, Ministry of Social Affairs and Health, Government of secondary use of health and social data, 552/2019. The EU General Data Protection Regulation (GDPR) provides grounds for processing that are in the legitimate interests of data controllers or necessary for public interest, including serious cross-border threats to health.

35. World Economic Forum, "APPA – Authorized Public Purpose Access: Building Trust into Data Flows for Well-being and Innovation", White Paper, 2019.

36. This guideline from Japan's Ministry of Internal Affairs and Communications, along with the "Security Management Guideline for Information Processing Providers Dealing with Medical Information" from the Ministry of Economy, Trade and Industry, and the "Guideline for the Security Management of Medical Information Systems" from the Ministry of Health, Labor and Welfare, are collectively referred to as the "Three Guidelines from Three Ministries" (see Google Cloud, https://cloud.google.com/security/compliance/3g3m).

37. The Act on Securing Quality, Efficacy and Safety of Pharmaceuticals, Medical Devices, Regenerative and Cellular Therapy Products, Gene Therapy Products, and Cosmetics (PMD Act), November 2014.

38. Moorthy, Vasee, et al., "Data sharing for novel coronavirus (COVID-19)", *Bulletin of the World Health Organization*, vol. 98, no. 3, 2020, https://www.who.int/bulletin/volumes/98/3/20-251561/en/.

39. See Lopez-Gonzalez, Javier and Francesca Casalini, "Trade and Cross-Border Data Flows", OECD Trade Policy Papers, no. 220, 2019, for an overview and discussion on transfer mechanisms.

40. Although these adequacy decisions are currently limited in terms of countries, the number of users covered is wide, resulting particularly from the EU-US Privacy Shield adequacy and the EU-Japan reciprocal adequacy.

41. Organisation for Economic Co-operation and Development (OECD), "Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data", 2013, referenced in United States-Mexico-Canada Agreement Article 19.8.

42. Association of Southeast Asian Nations (ASEAN), "The 18th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN)", 2018.

43. See the Case study: Smart and connected industries, included in this paper.

44. Government of Australia, Department of Foreign Affairs and Trade, "Australia-Singapore Digital Economy Agreement", 2020, https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement.

45. World Trade Organization, "DS413: China – Certain Measures Affecting Electronic Payment Services", 2012.

46. The two-tier test established under GATT XX also applies to GATS general exceptions according to World Trade Organization, "DS285: United States – Measures Affecting the Cross-Border Supply of Gambling and Betting Services", 2005.

47. WTO, General Agreement on Trade in Services Annex on Telecommunications, Article 5, "Access to and use of Public Telecommunications Transport Networks and Services".

48. World Trade Organization, Services: Agreement, "Understanding on Commitments in Financial Services", https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm.

49. Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) Article 14.11, "Cross-Border Transfer of Information by Electronic Means", https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/tpp-ptp/text-texte/14.aspx?lang=eng.

50. CPTPP Article 14.13, "Location of Computing Facilities".

51. CPTPP Article 14.17, "Source Code"; Amendment for algorithms in the "Agreement between the United States of America and Japan concerning digital trade", Article 17, https://ustr.gov/sites/default/files/files/agreements/japan/Agreement_between_the_United_States_and_Japan_concerning_Digital_Trade.pdf; United States-Mexico-Canada Agreement, Chapter 19 "Digital Trade", Article 19.16, https://ustr.gov/sites/default/files/files/agreements/FTA/ / Text/19-Digital-Trade.pdf.

52. CPTPP Article 14.3, "Customs Duties".

53. See a comparison in World Economic Forum, "Exploring International Data Flow Governance", White Paper, 2019.

54. Gasser, Urs, "Interoperability in the Digital Ecosystem", Berkman Klein Center for Internet & Society, Harvard University, Research Publication no. 2015-13, 2015.

55. The European Union General Data Protection Regulation (GDPR) defines even metadata without an obvious identifier as personal data as it can lead to identification combined with other data. Such protection of metadata (or binding laws specific to the protection of personal information) lacks direct equivalents under, for example, US Federal or Chinese national laws. Also, Australian privacy rules do not define all metadata as personal information, as determined in the Ben Grubb vs Telstra Corporation court decision in 2015.

56. An example of such interpretation of mixed data sets is found in EU law ("Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union", 29 May 2019, https://ec.europa.eu/digital-single-market/en/news/guidance-regulation-framework-free-flow-non-personal-data-european-union).

57. Examples of sectoral implementation include Korea (financial services), China (several sectors), Philippines (banking), Australia (medical data) and Turkey (online payments).

58. See the EU "White Paper on Artificial Intelligence: A European approach to excellence and trust", 2020; source code disclosure is required under cybersecurity and "secure and controllable" policies in several countries.

59. United Nations Conference on Trade and Development (UNCTAD), "Summary of Adoption of E-Commerce Legislation Worldwide", 2020, https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx.

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