DFFT:

Paths Towards Free and Trusted Data Flows

WORLD ECONOMIC FORUM

Summary:

Turning the DFFT vision into policy action

In his landmark speech at the Annual Meeting of the World Economic Forum in Davos-Klosters in January 2019, Prime Minister Abe invited leaders "to build an international order for *Data Free Flow with Trust* (DFFT)". Leaders at the Forum's Annual Meeting in January 2020 provided multistakeholder inputs to the Osaka Track – a collective term for global governance processes needed to realise 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.

Our economies are increasingly data-driven as we move towards Society 5.0. International trade, industrial production and societal functions increasingly depend on efficient access to data, while the cost of data restrictions are also increasing. The future of manufacturing with smart and connected industries, as well as the importance of data to tackle challenges such as pandemics and aging societies, highlight 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 were few similarities between two legal systems. Nonetheless, there is a fundamental gap on the free flow of non-personal information due to diverging definitions, regulatory approach (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 for individual control rights for their personal information in accordance with international guidelines and standards. They should also ensure the availability of multiple mechanisms and derogations for 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 including, for example, by 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 support and stress the importance of global, market-led, voluntary and consensus-based standards developed by multistakeholder forums involving non-governmental actors, and acknowledging such efforts at intergovernmental forums like 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 JSI negotiations at the WTO) 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; prohibit requirements to localise 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 GATS-consistent, non-discriminatory basis for like conditions.
- Many restrictions are currently imposed as forced joint-ventures (through foreign equity caps), technology transfer or ex ante licensing requirements for establishing data centres, engage in data collection and provision of 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 organisations 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 larger industry actors should also forge public-private partnerships to advise MSMEs on using digital technologies to drive growth and competitiveness and the ability to reach new markets.

DFFT and the Osaka track

Although we are more than two decades into the era of digitalisation, it is continuing to transform the global economy and our societies by bringing our markets and people closer to each other. There are more internet-connected devices than the number of people in the world. By 2023, there will be 29.3 billion networked devices, 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 the essential functions in our society. Yet, domestic rules governing data are increasingly divergent, restrictive and disruptive to global trade, 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 restrictive policies have doubled in the last ten years.[2]

Timely, 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 Annual Meeting of the World Economic Forum at Davos-Klosters in January 2019, Prime Minister Abe invited leaders "to build an international order for *Data Free Flow with Trust* (DFFT)"–[3] a vision where openness and trust exist in symbiosis, and not as contradictions. At the same Annual Meeting, 76 countries launched new negotiations on digital trade, the so-called ongoing Joint Statement Initiative (JSI) on e-commerce.[4]

Legacy of 2019 G20 summit and the Osaka Track

In June that same year, G20 Trade and Digital Economy Ministers at Tsukuba under Japan's chairmanship, stressed the significance of cross-border data flow 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, the Heads of Governments agreed to work towards the DFFT vision. The Osaka Leaders' Declaration states that legal frameworks – both domestic and international – should be respected. At the same time, we must enhance the interoperability between each framework to allow data to flow more freely.[6] The world

---

[1] Cisco, VNI Global Fixed and Mobile Internet Traffic Forecasts, 2018

[2] ECIPE, Digital Trade Estimates, 2018

[3] Speech by PM Abe Shinzo at WEF Annual Meeting at Davos-Klosters, "Toward a new era of hope driven economy", January 23, 2019. Accessed at: https://www.weforum.org/agenda/2019/01/abe-speech-transcript/

[4] Joint Statement on electronic commerce, WT/L/1056, January 25, 2019

[5] G20 Ministerial Statement on Trade and Digital Economy, June 9, 2019. Accessed at: https://www.meti.go.jp/press/2019/06/20190610010/20190610010-1.pdf

[6] G20 Osaka Leaders Declaration, June 29, 2019. Accessed at: https://www.mofa.go.jp/policy/economy/g20_summit/osaka19/en/documents/final_g20_osaka_leaders_declaration.html

leaders also agreed to the *Osaka Track* – a collective term for global governance processes needed to unleash the benefits of more open and trusted dataflows.

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 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 realise 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.

[7] Gasser, Urs, "Interoperability in the Digital Ecosystem". Berkman Center for Internet & Society, Harvard University, Research Publication No. 2015-13, July 6, 2015.

Towards a data-driven economy

The digital economy (supported by data flows) makes up a sizable 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 still growing six times faster than major emerging markets on an average.[8]

Digitalisation has also supported a 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.

For example, developing countries account for 38% of services trade, and the share is rapidly outpacing that of developed economies.[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 also key ingredients for industrial production. In terms of value, these tools account for 5 to 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, while 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.

---

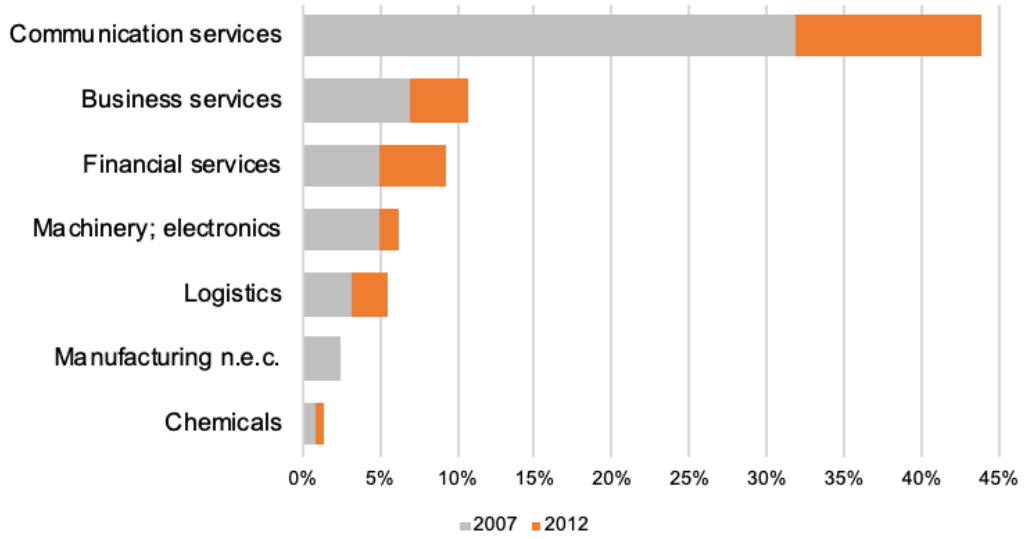
[8] UNCTAD, Digital Economy Report, 2019 estimates show up to 15.5% of global GDP is predominantly generated by business-to-business (B2B) digital activities. According to eMarketer, Worldwide Retail and Ecommerce Sales, 2018, the turnover of e-commerce transactions alone was US$2.7 trillion in 2017 and growing 25% per year. US Bureau of Economic Analysis estimated the digital economy to account for 6.9% of US GDP ($1.35 trillion) in 2017.

[9] UNCTAD, International Trade in ICT Services and ICT-Enabled Services, October 2015; see also Nicholson, Noonan. Digital Economy and Cross-Border Trade: The Value of Digitally Deliverable Services, 2017

[10] UNCTAD, Handbook on Services, 2019

[11] ITC, Unlocking Markets for Women to Trade, 2015; Digital Economy Unlocks Doors for Women Entrepreneurs in Africa, 2016

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



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

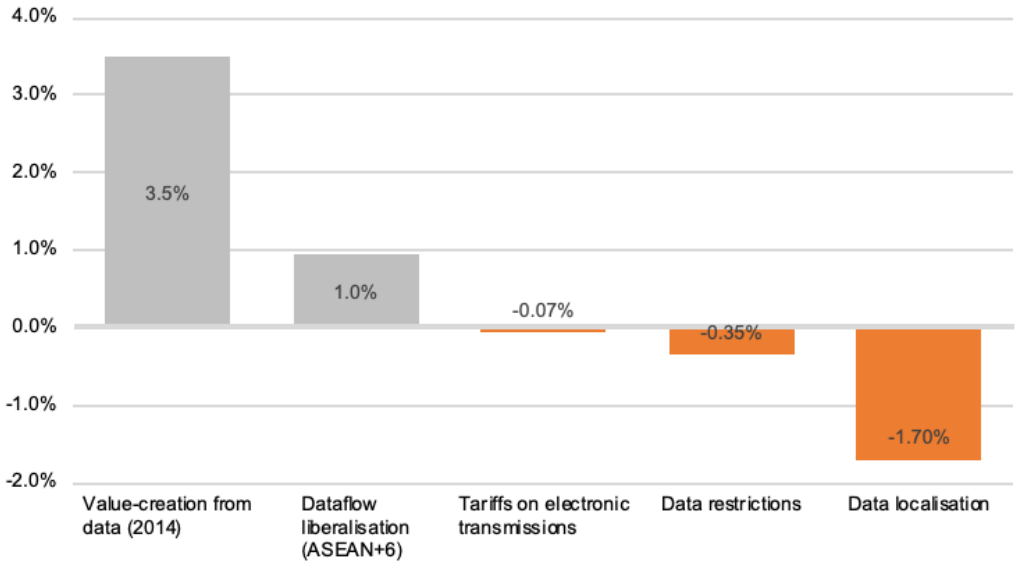
The cost of data restrictions

If efficient use of data and connectivity is a significant productivity-enhancing tool available 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 (such as motor vehicles, machinery, medical and scientific equipment) generate or transmit some form of data, which are routinely stored at one central location globally or regionally.[12]

Regulatory conditions or requirements on transferring data, and in particular data localisation policies – i.e. regulatory requirements to store or process data locally – are major trade frictions. Such obligations force exporters to build or lease data centres in every country of operation, imposing prohibitively high compliance and entry costs. Evidence shows that these requirements hamper economic growth in the countries that impose them and undo the gains harnessed from digitalisation.

[12] Rentzhog, No transfer, no production, National Board of Trade of Sweden, 2014

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



Source: McKinsey/Telegraphy 2017; USITC, Evenett, Lee-Makiyama, 2020 (forthcoming); ECIPE, 2013; 2019;

- Cross-border data flows added US$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] US International Trade Commission (USITC) estimates the productivity gains from data flows were approximately 3.4 to 3.5% of GDP in the United States.[14]
- Liberalising data flows and e-commerce among all members of the Regional Comprehensive Economic Partnership (RCEP) could increase regional GDP by up to 1%.[15]
- Discriminatory tariffs on electronic transmissions generate losses for the local industry and government that are fifty times larger than the claimed tariff revenues.[16]
- Current data flow restrictions and data localisation requirements of some countries lower their GDP by up to 0.4 and 1.7 percent respectively, depending on the economy and severity of the measure.[17]
- A study conducted on three developing countries (in South America, South-East Asia and Africa) indicate that data localisation measures on IoT applications and M2M data could cut 59-68% of their productivity and revenue gains. Such losses of competitiveness lead also to a reduction of 4 to 5 billion USD in investments and 182,000 to 372,000 jobs – without any obvious benefits for privacy or local businesses.[18]

[13] McKinsey Global Institute, Digital Globalization: New Era of Global Flows, 2016, using data provided by Telegraphy
[14] USITC, Digital Trade in the US and Global Economies, 2014
[15] Forthcoming study by Evenett, Lee-Makiyama.
[16] Lee-Makiyama, Naranayanan, The Economic Losses from Ending the WTO Moratorium on Electronic Transmissions, ECIPE, 2019
[17] ECIPE, 2014; 2015
[18] Forthcoming study by GSM Association (GSMA).

Experts universally agree data localisation requirements have little positive impacts on jobs or security since the productivity losses exceed the minuscule number of jobs created in data processing. Also, 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 localisation requirements could lower companies' ability to ensure cybersecurity or consumer protection, and instead increase entry points for cyberattacks. The Financial Stability Board (FSB) has also warned that data transfer restrictions could actually limit regulatory oversight.[20]

[19] World Economic Forum, "Exploring International Data Flow Governance," December 2019.
[20] Financial Stability Board (FSB), FSB Report on Market Fragmentation, June 2019

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 we have seen (figure 1), data usage in industrial production is rapidly increasing, with a 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 1000 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 AI to optimise 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.

There are already national strategies and visions – such as Germany's "Industrie 4.0" or Japan's "Connected Industries" – of connecting humans, machines and technologies across borders into systems that will continuously create value. For example, the Connected Industries' framework is designed to magnify Japan's national strengths in terms of skills, existing technologies, 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-government 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 by themselves.

For example, the joint-technical committees of the International Organization for Standardization (ISO) and 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), governance implications (ISO/IEC AWI 38507) as well as various standards on trust, risk management and ethics on artificial intelligence.[22] .

National standard-setting bodies are members of ISO and IEC, but often influential on their own, bringing together local and international actors. Entities like NIST (National Institute of Standards and Technology) in the US, JISC in Japan, DIN in Germany; or Cenelec and ETSI within the EU are such examples. In addition, there are also sectorial or professional standard setting bodies relevant for the future of manufacturing, such as 3GPP (of primarily networks vendors, for mobile network and 5G standards), IEEE (of engineers with an emphasis on electronics and computing).

Some governments may pursue industrial policies with an objective to create 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 serve as motivation for these initiatives. In time, such policies could impose a *de facto* prohibition of cross-border transfer of data, use of foreign algorithms or applications, or mandatory disclosure of source codes.[23]

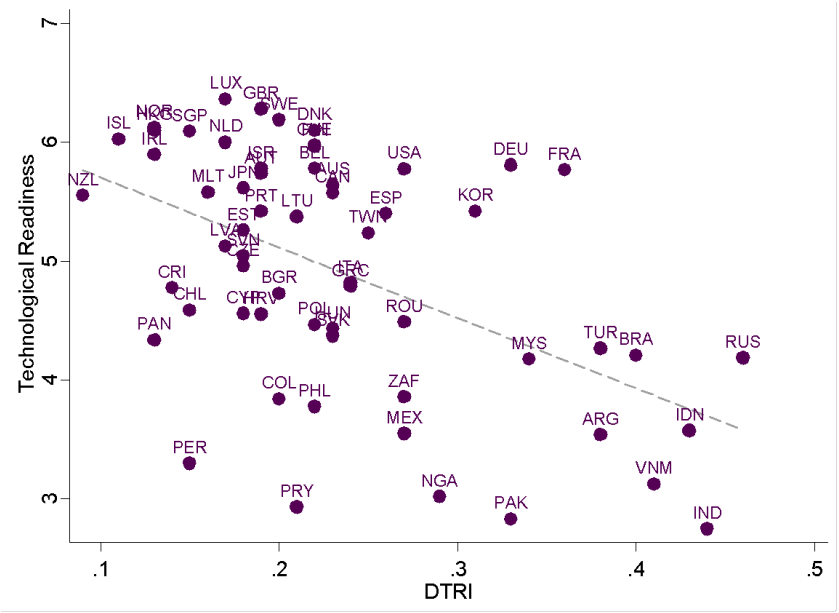
---

[21] The rapporteur thanks Michitaka Nakatomi, Special Advisor, JETRO, Consulting Fellow, RIETI, and Dr Urs Gasser, Executive Director, Berkman Klein Centre for Internet & Society, Professor, Harvard Law School for their valuable inputs.

[22] ISO/IEC JTC 1/SC 42 is currently developing various artificial intelligence related standards, such as Frameworks for AI Systems using Machine Learning; Risk Management; Overview of Trustworthiness, Governance Implications of the Use of AI by Organizations. Accessed at: https://www.iso.org/committee/6794475/x/catalogue/p/0/u/1/w/0/d/0

[23] World Economic Forum, Global Competitiveness Report, 2017; Economic Research Institute for ASEAN and East Asia (ERIA), 2020.

Figure 3: A country's ability to adapt new technologies for production (vertical axis) correlates with digital restrictiveness (horizontal axis).



Source: World Economic Forum, 2017; ECIPE, 2018

Current restrictions on foreign ownership in business-to-business industries or intellectual property rights (IPR) issues (like forced transfer or technologies or patent-trolling) also impact the uptake of innovative industrial technologies. Research shows how restricting data use is not just an impediment on trade, but also 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.

Broader societal benefits of data

Not all values of digitalisation are captured in purely economic terms. Just as concepts like *Industry 4.0* highlight the digital transformation of manufacturing, *Society 5.0* underscores how digitalisation could tackle today's social challenges and usher broader transformation, rather than just within industrial production.

Our societies have evolved from hunter-gatherer (1.0), agrarian (2.0), industrial (3.0) and reached today's information-based (4.0) arrangements. We are 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 optimise entire societal and welfare systems – and not just businesses – that tend to people's needs at the time and the place where needed, tailored to the individual to improve their quality of life. For example:

- Reuse of data and sharing between government entities as appropriate to tackle ageing society and public health challenges with more accurate preventive care, mitigating increasing costs.
- Free data flows can help address pollution, climate change and other sustainability objectives by minimising waste and increasing traceability across sustainable supply chains.
- Efficient and open access to data is essential for tracking and enabling the delivery of many Sustainable Development Goals (SDGs).

Open access to public data plays a central role in this area. Data collaborations have been set up to facilitate 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 stocks monitoring), responding to natural disasters and other areas of public policy or civil contingency planning.[24] These initiatives are not without challenges, however, including those created by a lack of legal uncertainty created by market regulators – underscoring the importance of improving DFFT governance.

Digitalisation 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, policymakers must take a human-centric approach to data governance – an approach that is advocated by philosophies like governance innovation.[25] Future policies must be agile, risk and outcome-based, as domestic regulators and international cooperation will never keep pace with the rate of innovation. New technologies could also achieve better outcomes and compliance than sanctions-based models.

[24] GovLab. Data Collaboratives Explorer. Accessed at: https://datacollaboratives.org/explorer.html
[25] Study Group on a New Governance Models in Society 5.0, Governance and laws in the age of Society 5.0, 2020. Accessed at: https://www.meti.go.jp/english/press/2019/pdf/191226001.pdf

Case study:[26] Data in the service of public health

Countries around the world are increasingly faced with the challenges of delivering affordable healthcare for their citizens. Data-driven technologies are increasingly at the centre of healthcare solutions, including aggregating and sharing of physiological and medical data, healthcare-site details and infection information.[27]

For example, efficient data collection and open access to data are instrumental for more rapid treatments provided at home, preventive examinations and early detection of diseases. Personalised 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 on 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 cease 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.[28]

Aggregating genomic, phenotypic and clinical data at a global scale can improve diagnoses and paths to treatment.[29] For example, sharing clinical trial data can lead to new discoveries and strengthen trial results,[30] especially for the development of "orphan drugs" against rare diseases that affect 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 sub-national health data management systems.[31] 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.[32]

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, 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.[33]

A best practice for regulating healthcare data is Japan's Next-Generation Medical Infrastructure Law, which creates a voluntary nationwide system of anonymised patient treatment and outcome records available for trusted and approved medical and healthcare R&D purposes.[34] Similarly,

---

[26] The rapporteur thanks Dr Hiroaki Miyata, Professor, Keio University School of Medicine for his valuable inputs for this section.

[27] "Society 5.0, Examples of Creating New Value in the Field of Healthcare and Caregiving". Accessed at: https://www8.cao.go.jp/cstp/english/society5_0/medical_e.html.

[28] Forbes, AI and Healthcare: A Giant Opportunity, February 11, 2019

[29] "Global Data Access for Solving Rare Disease: A Health Economics Value Framework". Accessed at: https://www.weforum.org/reports/global-access-for-solving-rare-disease-a-health-economics-value-framework

[30] "Data anonymisation – a key enabler for clinical data sharing", Workshop Report. Accessed at: https://www.ema.europa.eu/en/documents/report/report-data-anonymisation-key-enabler-clinical-data-sharing_en.pdf

[31] WHO Guideline, Recommendations on Digital Interventions for Health System Strengthening, https://apps.who.int/iris/bitstream/handle/10665/311941/9789241550505-eng.pdf?ua=1.

[32] Modjarrad K, Moorthy VS, Millett P, Gsell P-S, Roth C, Kieny M-P (2016) Developing Global Norms for Sharing Data and Results during Public Health Emergencies. PLoS Med 13(1): e1001935

[33] World Economic Forum, "Federated Data Systems: Balancing Innovation and Trust in the Use of Sensitive Data, July 2019

[34] Government of Japan, Act Regarding Anonymised Medical Data to Contribute to R&D in the Medical Field" ("Next Generation Medical Infrastructure Act", May 12, 2017)

Finland's secondary use of health and social data permits the use of healthcare data for purposes other than the primary reason (in accordance with EU GDPR).[35] Leading researchers have also gathered to outline a set of principles for "Authorized Public Purpose Access (APPA)" that recognises exceptional conditions during which requirements for consent and anonymisation might be waived under emergencies deemed important for public safety or protection of human life.[36]

Japan's set of security management guidelines for "Cloud Service Providers in Handling Medical Information" set an example for how third-parties can certify security requirements.[37] A revised pharmaceutical law (the Pharmaceutical, Medical Devices Act) also came into effect in 2014,[38] 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.[39]

[35] Ministry of Social Affairs and Health of Finland, Government of Secondary use of health and social data, 552/2019. 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.

[36] World Economic Forum, APPA – Authorized Public Purpose Access: Building Trust into Data Flows for Well Being and Innovation, December 2019

[37] The guidelines from the Ministry of Health, Labour and Welfare, along with the "Security Management Guidelines for Information Processing Providers Dealing with Medical Information" from the Ministry of Economy, Trade and Industry, and the "Security Management Guidelines for Cloud Service Providers Handling Medical Information" from the Ministry of Internal Affairs and Communications, often collectively referred to as the "Three Guidelines from Three Ministries."

[38] 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 25, 2014

[39] Moorthy et al, "Data Sharing for Novel Coronavirus (COVID-19). Accessed at: https://www.who.int/bulletin/volumes/98/3/20-251561/en/

The architecture for data governance

The *Osaka Track* is a process to promote efforts on international rule-making for 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 or 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, where each forms 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 categorised 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 other jurisdictions make a distinction between domestic and foreign entities for data that is perceived to pertain to national security, or designate specific entities as either trusted, or of particular high risk – where some jurisdictions also routinely categorise all data as being sensitive.

Figure 4: The architecture for data governance involved in the Osaka Track

	Relevant pillars for international cooperation on data flows			
	Transfer mechanisms	**Legal & regulatory cooperation**	**Technical cooperation**	**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 harmonisation (Budapest Convention)	Standard-setting in multi-stakeholder forums (ISO/IEC, IEEE, 3GPP, among others)	WTO rules (case law, GATS and Reference Paper and Annex on Telecommunications) with privacy and other exceptions, along with two-tier test (for least-trade restrictiveness and necessity) Ongoing WTO JSI negotiations
Limited participation	Adequacy decisions to jurisdictions with adequate protection, e.g. EU-Japan reciprocal adequacy, EU adequacy for US Privacy Shield. Certification programmes (under government oversight), e.g. APEC CBPR "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 MLATs 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 DEA)	National and regional standard-setting, such as UNECE Exclusive "data spaces" initiatives and consortium. Bilateral mutual recognition agreements (MRAs) or equivalence decisions	Digital trade commitments (e.g. data flow, prohibition on localisation and source code access disciplines derived from CPTPP) developed in Japan-US, USMCA, EU texts, DEPA, with varying exceptions

At the outset, before there is any international cooperation, 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.[40] Notably, many jurisdictions acknowledge user consent, contractual reasons or public and legitimate interests as a derogation to a prohibition to overseas transfer of personal information. Governments may also pre-authorise 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.[41] 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

[40] See Lopez-Gonzalez, Casalini, Trade and Cross-Border Data Flows, OECD, 2019 for an overview and discussion on transfer mechanisms

[41] Although such 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 Japan-EU reciprocal adequacy.

is transferred abroad. Although the certification process may allow for self-certification, relevant government agencies guarantee enforcement of compliance.

Legal and regulatory cooperation comprises intergovernmental efforts for best practice, common normative principles and even goes toward harmonisation of domestic laws. Notably, the OECD has developed detailed guidelines on privacy legislation that encourage harmonisation of domestic regulations amongst its members in this area, which is also referenced in some trade agreements.[42] 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.[43]

In the area of law enforcement, the Budapest Convention under the Council of Europe (COE) has 67 signatories, including non-members of COE from outside Europe. In the first instance, signatories have agreed to designate certain acts 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 standardisation and industrial cooperation* that usually take place in wider and multi-stakeholder forums. For example, the IEEE or the joint-technical committees of the International Organization for Standardization and International Electrotechnical Commission (ISO/IEC) develop standards and best practices to facilitate technology interoperability, while 3GPP sets the standards for the telecommunication industry.[44] 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 instruments include diplomatic instruments and strategic partnerships, such as the recent Digital Economy Agreement (DEA) between Australia and Singapore,[45] with associated memoranda of understanding (MoUs) on data innovation and artificial intelligence.

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 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.[46] Invoking privacy exceptions to those commitments would be also subject to conditions.[47]

---

[42] OECD, Recommendation of the Council concerning Guidelines governing the Protection of Privacy and Transborder Flows of Personal Data, 2013, referenced in USMCA article 19.8.
[43] ASEAN, The 18th ASEAN Telecommunications and Information Technology Ministers Meeting (TELMIN), December 2018
[44] See also the case study above on smart and connected industries.
[45] Australia-Singapore Digital Economy Agreement, 23 March 2020: https://www.dfat.gov.au/trade/services-and-digital-trade/Pages/australia-and-singapore-digital-economy-agreement
[46] *China*—Certain Measures Affecting Electronic Payment Services, DS314.
[47] Two-tier test established under GATT XX also applies to GATS general exceptions according to *United States*—Online Gambling, DS285.

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.[48] 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.[49]

More recent trade rules include the Comprehensive and Progressive Trans-Pacific Partnership (CPTPP) concluded in 2017 between eleven countries. The CPTPP contains core commitments that are essential for DFFT including provisions on cross-border transfer of information,[50] prohibition of data localisation as a condition for conducting business,[51] limits on the mandatory disclosure of source code (later amended with algorithms),[52] and a ban on the imposition of customs duties on electronic transmissions.[53]

Later trade agreements build on these provisions and their exceptions. Notably, USMCA and the Japan-US Digital Trade Agreement incorporates information transfer for financial services and more specific commitments on algorithms or privacy.[54] The Digital Economy Partnership Agreement (DEPA) between Chile, New Zealand and Singapore; and recent EU FTA negotiating texts contain 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 – is critical to the Osaka Track. The notion of interoperability is also central for trust and openness since it can foster trust through all the pillars of the Osaka Track. In turn, trust encourages greater investment in interoperability as well as the necessary institutional structures that allow data to be shared appropriately and securely.. 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.[55]

Openness and interoperability today is conditioned on efficient cooperation where governments, business 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. So too, jurisdictions that share similar legal concepts, offer effective enforcement and recourse to address any negative externalities arising from data flows between them, and hence 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.

---

[48] GATS Annex on Telecommunications, article 5
[49] Understanding on commitments in financial services
[50] CPTPP article 14.11
[51] CPTPP article 14.13
[52] CPTPP article 14.17; amendment for algorithms in article 17 of Japan–US agreement concerning digital trade; article 16 of USMCA chapter 19.
[53] CPTPP article 14.3
[54] See a comparison in World Economic Forum, "Exploring International Data Flow Governance,"17 December 2019.
[55] Gasser, Urs, "Interoperability in the Digital Ecosystem". Berkman Center for Internet & Society, Harvard University, Research Publication No. 2015-13, July 6, 2015.

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 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, 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 or usernames, internet provider addresses, email) or network identifiers like phone numbers, MAC or IP-addresses as personal information, while other jurisdictions do not.[56] Similarly, vehicle identification numbers or serial numbers of devices, 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.[57]

Although many regulations are based on protecting certain data *subjects* – personal data that describe subjects, ie. 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 international transfer of any data that is held by financial institutions, online payment services, trading or business records and healthcare providers.[58]

New legislation may even discriminate against data objects of foreign origin – such as algorithms or applications – from being used in a country without prior authorisation. Certain governments grant themselves access proprietary source codes for software and AI-algorithms.[59] There are also examples for *ex ante* licensing requirements for collecting relatively simple data, such as data for autonomous driving or e-commerce activities.

---

[56] European Union General Data Protection Regulation (GDPR), which defines even metadata without an obvious identifier as personal data as they may lead to identification combined with other data. Such protection of metadata (or binding laws specific to protection of personal information) lack direct equivalents under e.g. US Federal or Chinese national laws. Also, Australian privacy rules do not define all metadata as personal information, as determined in the *Grubb v. Telstra* in 2015.

[57] 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, May 29, 2019)

[58] Examples of such sectoral implementation include Korea (financial services); China (several sectors); Philippines (banking); Australia (medical data), Turkey (online payments).

[59] See EU White Paper on Artificial Intelligence – A European approach to excellence and trust, February 19, 2020; source code disclosure required under cybersecurity and "Secure and Controllable" policies in several countries.

Recommendations for advancing the Osaka track

Discussions with WEF stakeholders on realising the DFFT vision identified many forums, pillars and levels of cooperation that shapes 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 Osaka Track (figure 4) illustrates how pathways to free and trusted data flows are possible among various configurations. However, the architecture can be improved upon, and the mapping process has also revealed crucial gaps.

The Osaka Track needs to fill these gaps in all pillars and levels of cooperation, recalling 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 flow would reverse the benefits gained from connectivity and digitalisation. 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 64% of 107 countries to date have enacted privacy laws or privacy protections and only 52% of 125 countries have online consumer protection laws – with lags in many least developed countries.[60] In some cases, debates are ongoing regarding new laws, in others the conversation still centres on achieving connectivity for those not yet online.

The following lays out recommendations for advancing 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 practice of safeguard and accountability mechanisms currently available. The principle offers hope that the Osaka Track can be advanced at a global scale, as well as with variable geometry – in a regional context or amongst groups of like-minded countries.

On personal information and transfer mechanisms

- Governments should adopt good privacy and security protections that empower users for individual control rights for their personal information in accordance with international guidelines and standards. Stakeholders have particularly noted the importance of OECD Privacy Framework and APEC Privacy Framework. Businesses should support increased consumer trust by proactively establishing it with clients and users including, for example, by providing information on data treatment and enhancing transparency.
- Transfer mechanisms are essential since data becomes otherwise subject to *de facto* localisation. This report has outlined several transfer mechanisms that allow for 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,

[60] UNCTAD, Summary of Adoption of E-commerce Legislation Worldwide (webpage). Accessed at: https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Global-Legislation.aspx (Accessed 30 March 2020)

therefore, ensure the availability of multiple mechanisms and derogations for cross-border transfer of personal data on a non-discriminatory basis for like conditions.

- Those jurisdictions who apply unilateral or reciprocal adequacy decisions should be encouraged to expedite such decisions and base them on well-defined and transparent criteria according to procedural fairness.
- Certification programmes like APEC CBPR or 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 for these systems, especially for the developing countries outside of 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 recognise the importance of non-personal data and M2M-communications to the growth of the global economy and should refrain from restricting its cross-border flow. Many stakeholders agreed that such data, or data that is anonymised, pseudonymised, protected or publicly available, is not personal information.
- A clear area for law enforcement and legislative cooperation is in the area of 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 Mutual Legal Assistance Treaties (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 relates to the function the public authority exercises.

On standardisation and technical cooperation

- Stakeholders support and stress the importance of global, market-led, voluntary and consensus-based standards developed by multistakeholder forums involving non-governmental actors, and acknowledging such efforts at intergovernmental forums like 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 such 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. Such dialogue should bring together experts from different spheres – including trade policy makers, data protection regulatory, 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 to conform standards on industrial data.

- Beyond targeted government-to-government engagement, policymakers 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 publication of impact assessments to ensure the appropriateness and effectiveness of regulatory approaches; and are targeted, 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.

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 the trust between different parties.
- Specifically, many recent trade agreements already include provisions that facilitate data flows across borders; prohibit requirements to localise 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 (CPTPP, USMCA, Japan-US Digital Trade Agreement, DEPA) have further specified commitments on new emerging technologies.
- 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 restrictions are currently imposed as forced joint-ventures (through foreign equity caps), technology transfer or *ex ante* licensing requirements for establishing data centres, engage in data collection and provision of 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.

What governments can do for development

- Developed economies, international organisations 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 digitalisation 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 with a view to facilitating data transfers so compliance costs and complexity do not hinder developing countries and MSMEs from participating in global trade.

- Governments and larger industry actors should also forge public-private partnerships to advise MSMEs on using digital technologies to drive growth and competitiveness and the ability to reach new markets.

Contributors

Steering Committee

Anabel Gonzalez, Non-resident Senior Fellow, the Peterson Institute for International Economics

Hiroaki Nakanishi, Executive Chairman, Hitachi Ltd

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

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

Ngozi Okonjo-Iweala, Non-resident distinguished Fellow, Brookings Institution

Paul Thomas Jenkins, Chair of the Board, OpenText Corporation

Richard Samans, Managing Director, Managing Board, World Economic Forum

Takahito Tokita, President and Representative Director, Fujitsu Limited

Experts Committee

Amitendu Palit, Senior Research Fellow, National University of Singapore

Annabella Ng, Head of Regional Strategy, Public Affairs, Grab Singapore

Austin Imperato, Manager, Government and Regulatory Affairs, IBM

Barbara Kotschwar, Senior Director, Global Government Relations, Visa Inc.

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

Chisato Amano, Expert, ICT and Policy Analysis, Global Public Policy Relations Office, NEC Corporation

Francois Martins, Head of Government Relations, Brazil, MercadoLibre

Haishan Fu, Director, Development Data, World Bank Group

Hiroaki Miyata, Professor, Health Policy and Management, Keio University School of Medicine

Ichiro Hara, Director, International Affairs Bureau, Keidanren

Jake Colvin, Vice-President, Global Trade Issues, National Foreign Trade Council

Javier Lopez Gonzalez, Senior Trade Policy Analyst, Organisation for Economic Cooperation and Development

Josh Kallmer, Executive Vice-President of Policy, Information Technology Industry Council

Joseph Whitlock, Director, Policy, Business Software Alliance

Julia Nielson, Deputy Director at Trade and Agriculture Directorate, Organisation for Economic Co-operation and Development

Jun Nakaya, Manager, Global Relations, Public Policy & Business Development Office, Fujitsu Limited; Chairperson of Trade Policy, JEITA

Lisa Pearlman, Head of Global Trade and International Policy, Apple

Martin Molinuevo, Senior Counsel, World Bank Group

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

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

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

Sadie Creese, Professor of Cyber-security, University of Oxford

Satoshi Yoshizawa, Senior Strategist, Technology Strategy Office, Hitachi

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

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

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

Usman Ahmed, Head of Global Public Policy, PayPal

World Economic Forum

Richard Samans, Managing Director, World Economic Forum

Sean Doherty, Head, International Trade and Investment

Kimberley Botwright, Community Lead, International Trade and Investment

Nivedita Sen, Trade and Investment Analyst

Rapporteur

Hosuk Lee-Makiyama, Director, ECIPE