FUTUREMATTERS™
CENTRE OF EXCELLENCE

SHAPING DATA POLICIES THROUGH **CROSS-BORDER COLLABORATION**

March 2024

CONTRIBUTOR:
Ivan Mortimer-Schutts
Advisor, Dataswyft

JAPAN FINTECH FESTIVAL™

SHAPING DATA POLICIES THROUGH CROSS-BORDER COLLABORATION

FUTUREMATTERS™
CENTRE OF EXCELLENCE

The Japan FinTech Festival 2024 (JFF) Roundtable on *"Shaping data policies through cross-border collaborations"* debated practical industry and policy issues related to the G7 Data Free Flow with Trust (DFFT) initiative. In December 2023, the G7 Digital Tech Ministers affirmed their intent to establish an Institutional Arrangement for Partnership (IAP) that will bring together data governance experts from governments, industry stakeholders, and data protection authorities, to contribute to the promotion of the cross-border flow of personal and non-personal data to operationalise DFFT. Participants at the JFF roundtable discussed practical business, legal and policy issues related to data transfer and sharing, in particular in the context of cross-border development of financial and digital services.

This paper provides context to the discussion and presents the main themes and viewpoints debated. The aim of this roundtable was to inform ongoing thinking about how industry and policymakers can collaborate effectively to better understand the market challenges we are facing and harness some emerging technologies and approaches as we seek to craft arrangements that can enhance data free flow between economies while preserving (or even strengthening) trust, integrity, and the equitable distribution of gains from digital economy trade and development.

Content

Introduction 04

Data Becoming Essential and Widespread in Market Development 06

Policy and Legislation is Evolving 10

The Potential of New Technologies, Infrastructure & Ecosystems 13

Recommendations & Considerations 15

References 18

Introduction

Digital economic development continues to expand the scope, complexity, and significance of data as a key - albeit abstract - ingredient in society and innovation. Individuals and data from and about them are at the heart of this evolution of the global digital economy. With the rise of digital platforms as motors of growth, cross-border trade in digital goods and services continues to expand. In both cases, whether it's related to our personal lives and online profiles, or to our roles representing companies and organisations, data increasingly exists online and often transcends national borders, legal jurisdictions, and organisational boundaries. Data is increasingly held in the cloud. Organisations are more aware of the diversity and value of data for various purposes. And data is increasingly essential to the application of machine learning and artificial intelligence.

The proliferating array and usage of data raises concerns about individuals' and companies' control over access to and usage of it by third parties. Policymakers and citizens are taking steps to enhance the legal rights of individuals to choose how their data is used and with whom it is shared, not just in a domestic setting but across jurisdictions. This raises questions about differences between not just in a domestic setting, but across jurisdictions regarding the rights and obligations of users, as well as the mechanisms and authority in place to enforce them. Governments have responded with new or modified data protection and privacy policies, as well as legislation.

Policymakers are also making an effort to enhance the flow and portability of data. These are often manifested in public interventions that aim to boost innovation, temper concentrated market power of incumbents and boost growth in new services. Domestic policies are proliferating in areas such as open finance, data portability, digital identity as well as digital trade measures in bilateral and regional trade agreements. These are important aims, especially in countries that may feel they could benefit more at home from digital development driven by companies in larger markets. At first glance, these aims may seem at odds with and difficult to reconcile with data protection, privacy, and localisation measures.

Diverging policy priorities have led individual jurisdictions to strike different balances between the interests of the state, private enterprises, and consumers. While governments may agree to some extent on high-level principles of data protection and mobility, on the ground, actual policy and legislative approaches and the application thereof, are leading to different outcomes that can be difficult to reconcile. Companies and individuals are increasingly faced with a fragmented landscape, handling data and consumer rights separately for different jurisdictions. Governments and industry need to coordinate efforts to develop inclusive governance arrangements that enhance the free flow of data if the potential of the digital economy is to be harnessed. This should not just be for incumbents, but more focused on fostering more equitable distribution of growth. Arrangements to foster trust, integrity, and control might develop around more decentralised ecosystems and new types of data intermediaries using consent-based systems and privacy-enhancing technologies. Regulation itself also needs to be codified in a machine-readable manner that enables complex compliance operations to be fulfilled in a world that will see increasing automation and use of machine learning and AI, not just to manage data sharing but also compliance.

The roundtable discussants included

- Dr David Hardoon, CEO Aboitiz Data Innovation
- Dr Nicola Jentzsch, Head of Innovation, Deutsche Bundesbank
- Hiroki Takahashi, Salesforce.com
- Hiroshi Nakatake, Managing Director, GLEIF Japan
- Jan Szilagyi, CEO, Toggle AI
- Robert Wardrop, Founder, CEO, RegGenome
- Daniel Nagy, Senior Business Analyst CBDC, Giesecke + Devrient
- Tiziana Sodano, Banca d'Italia

The roundtable was moderated jointly by

- Ivan Mortimer-Schutts, Advisor, Dataswyft
- Maiko Meguro, Japan Digital Agency

Data Becoming Essential and Widespread in Market Development

Data is diverse in its content, origins, structure, and usage. Effective policy and regulation of it both within and beyond a specific jurisdiction requires insights into and adaptation to specific contexts. The abstract, diverse and multi-faceted nature of data complicates the design of practical policy solutions to cross-border transfer and sharing of it. Features of data's production, usage and relationship to actual data subjects create varied contexts in which policy objectives are set and operational interventions designed. There are significant risks that regulations intended for one domain may overlap into or indirectly regulate data or domains outside of scope. Industry and policymakers at the roundtable agree that enhanced practical dialogue must inform the development of policy measures.

The concept of customer data as a distinct phenomenon is a recent development, and both companies and individuals are rapidly expanding their understanding and use of it. While digital platform companies may be 'native' to the data economy, other firms are only gradually enhancing their awareness and understanding of it. In the past, data was largely a by-product of other activities and was not readily captured, codified and easy to reuse. But the platform economy has expanded the production of data to a point at which the data profile has become a product. Understanding individuals' interests, actions, and behavior is valuable for informing and tailoring a wide range of activities, including sales and marketing, product design and distribution, as well as risk appraisal and monitoring. Leading digital companies exemplify this value. Their success is largely due to data-driven strategies, from targeted advertising to personalised financial services. This extends beyond advertising, with data and analytics significantly influencing financial innovation. Companies are accessing new data sources, like creditworthiness data or transaction patterns, to improve risk management across various domains, including anti-money laundering, investments, and payment processing. Furthermore, this data can be used to influence behaviour and belief, shaping consumer choices and financial decisions.

The value of data, albeit contextual, is now also being increasingly formalised. For digital platforms, it can be a primary source of revenue. Data storage and processing companies directly benefit from its proliferation, but indicators of consumer sentiment suggest a degree of dissatisfaction with how it is used and potentially also how the gains from harvesting and using it are distributed1. In parallel, governments are beginning to integrate the value of data into national accounts and statistics as well as explicit public sector interventions to enhance the mobilisation of data and consumer rights and controls over it2.

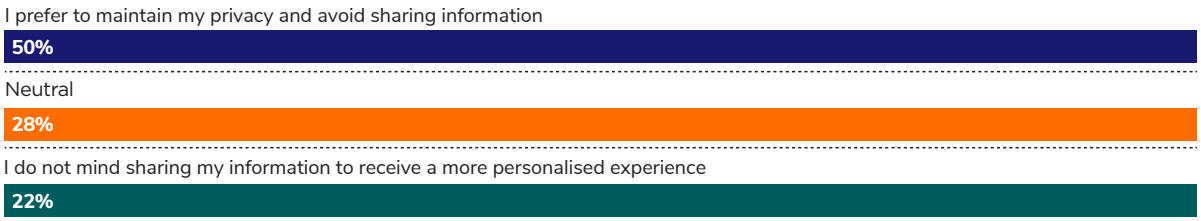
---

[1]The Oliver Wyman Forum's Global Consumer Sentiment Survey (2020) asked more than 67,000 people in 10 countries – Australia, Brazil, China, France, Germany, Italy, Mexico, Spain, the United Kingdom, and the United States – how they felt about sharing their information. https://www.oliverwymanforum.com/future-of-data/2021/jul/digital-consumers-value-data-transparency-and-privacy.html

[2]Refer to Coyle and Manley (2022) and the public initiatives, for instance, elements of the Data Empowerment and Protection Architecture (DEPA) in India and key EU regulations and policy interventions to support digital market development, data spaces and data governance.

Figure 1: Consumers Value Privacy Over Personalised Experiences

We asked people in 10 countries, "Which of the following best describes how you feel today?"



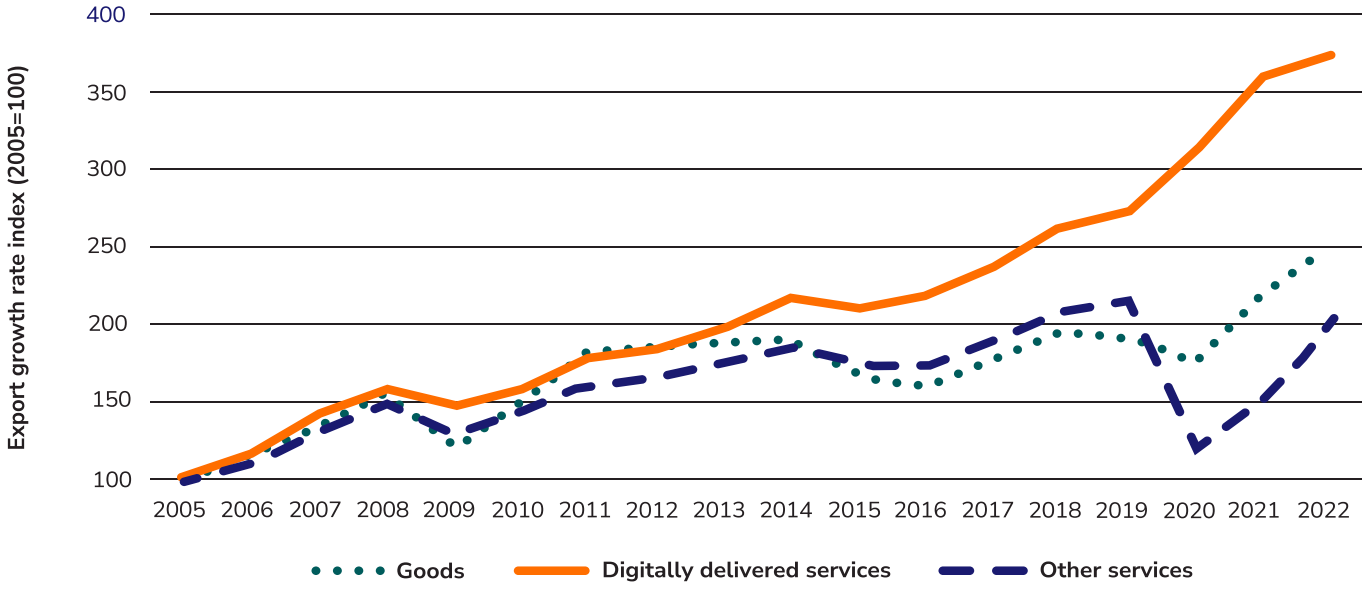
Source: Oliver Wyman Forum Global Consumer Sentiment Survey

Cross-border movement of and access to data is increasingly commonplace, yet ambiguous. Customers move and data moves with them – but the central platforms they keep it on may not. Businesses may draw upon data in one jurisdiction, analyse it via services in another and present or apply it in a third. Personal data might be prevented from moving, but be required to fulfil regulatory obligations. Zero-trust mechanisms may obviate the need to physically move data but still allow the analysis of it to provide the necessary insights or answers for other data-driven processes. It is also worth recalling that organisational or corporate data is intertwined with that of the officers that run companies, further blurring the boundaries and context in which personal data protection rules may operationally overlap with data sharing for legitimate business purposes. Organisations seeking certainty and clarity need to accept that this only comes with maturity. And as the market continues to evolve, certainty will not come soon. If we want zero risk, data will never move. Cross-border data regulation will have to manage the fluidity of implementations.

Continued growth of the value and sophistication of the digital economy will accentuate the issues at stake. Not least because of the pandemic, digital trade in its various guises has outpaced growth in trade in physical goods and other services. Companies are processing and storing data across borders for domestic needs. Digital platforms have expanded business operations across borders through virtually all modes of trade as defined by the WTO[3], putting increasing pressure on them to benefit where possible from economies of scale that often call for flexibility in where and how data is sourced, stored, and processed.

[3]Modes of trade refer to relation to location of trading parties and territories. Mode 1 refers to trade from the territory of one Member into the territory of any other Member (Cross border trade); Mode 2: in the territory of one Member to the service consumer of any other Member (Consumption abroad); Mode 3: by a service supplier of one Member, through commercial presence, in the territory of any other Member (Commercial presence); and Mode 4: by a service supplier of one Member, through the presence of natural persons of a Member in the territory of any other Member (Presence of natural persons).

Figure 2: Global exports of digitally delivered services have grown faster than exports of other goods & services



Source: WTO (2023b).

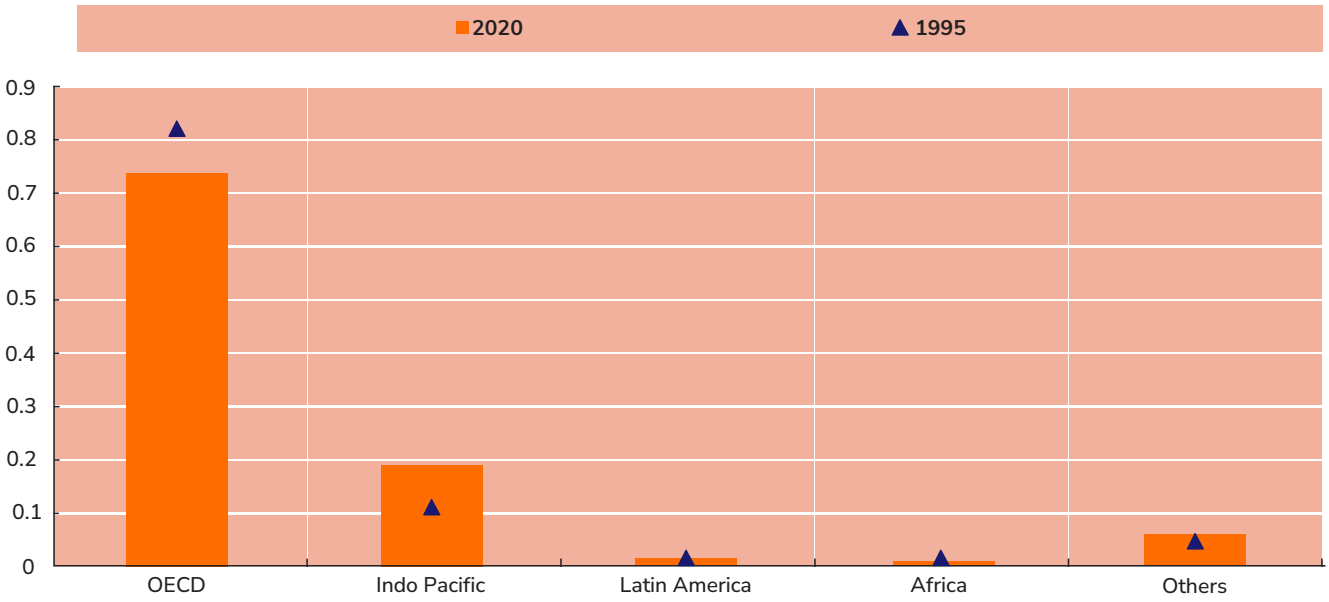
Note: The figure displays the growth rate of exports of good is 2005 (2005=100)

Broadening access to artificial intelligence and machine is likely to accelerate usage of data driven business models and value creation in the coming years. This will put further pressure on policymakers to clarify their aims and improve legislation and enforcement mechanisms or risk being overwhelmed and outpaced by market developments. There is growing uncertainty among industry providers not just about what the obligations are but how or if they would be enforced. To minimise risk, some companies shut down data exchange and take different approaches per country; meanwhile, other providers may be engaged in significant cross-border data processing beyond the jurisdiction and oversight of authorities. Infrastructure and services to process and consume data has so far lagged our capacity to produce it. The rise of AI is leading us to a 'Netflix moment' in which the scale of data usage and production may generate shifts in market structure and more granular distribution of sources of value creation across different jurisdictions.

Middle- and lower-income nations may have more at stake than developed economies shaping policy. The digital economy is growing especially rapidly in markets where new innovators have had fewer incumbents to displace or reform[4]. Many middle-income markets have seen long-term supply gaps in essential services like payments. These gaps have been filled not by banks or traditional payment service models dominant in advanced economies, but by new digital-native, non-financial platforms.

These platforms put data at the centre of their operations, allowing them to deliver cost-efficient services to mass-market consumers and businesses. Yet, these types of stakeholders and the countries in which they operate are often under-represented in the industry and multilateral forums shaping relevant policy and regulation.

Figure 3: Share of global digital trade exports by region



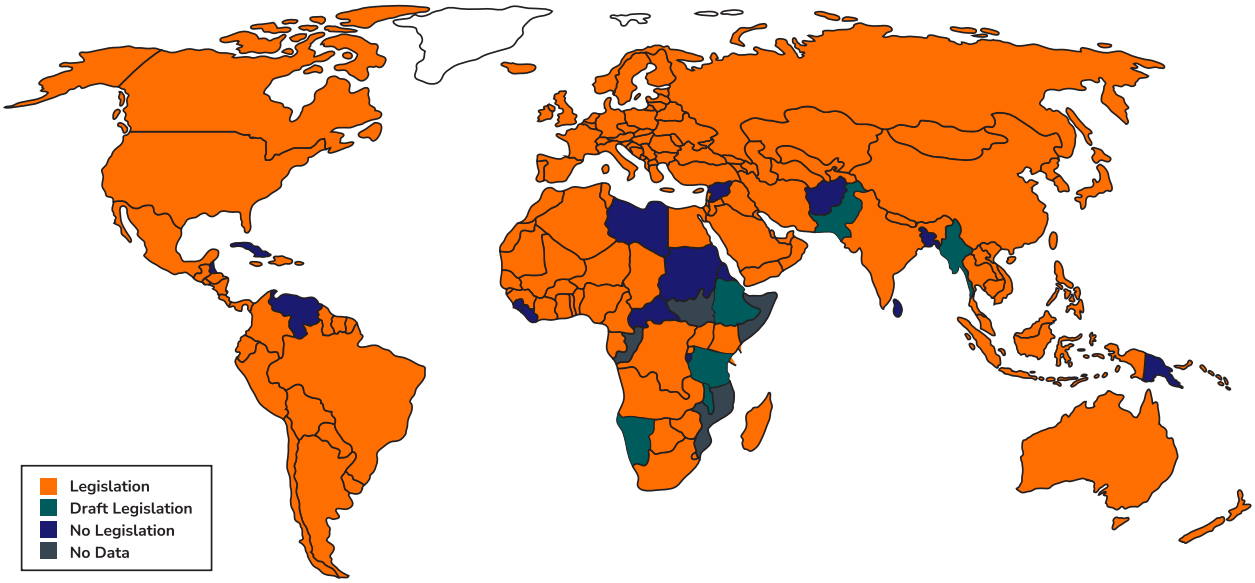
Note: Regions are mutually exclusive, so bars add up to 100%.
Source: Own calculations using OECD TiVA 2023 revision.

[4]See figure 3 that provides an indicator of the divergent rates of growth of digital trade by region.

Policy and Legislation is Evolving

Data protection and privacy legislation, digital and data market governance, digital trade agreements, as well as sector level schemes are playing catch up with markets. New data protection and digital competition authorities and regulations are gradually coming into place. Companies increasingly face a complicated, evolving patchwork of principles and laws, especially at the cross-border level. Authorities themselves face the challenge of enforcing compliance with new and modified legislation.

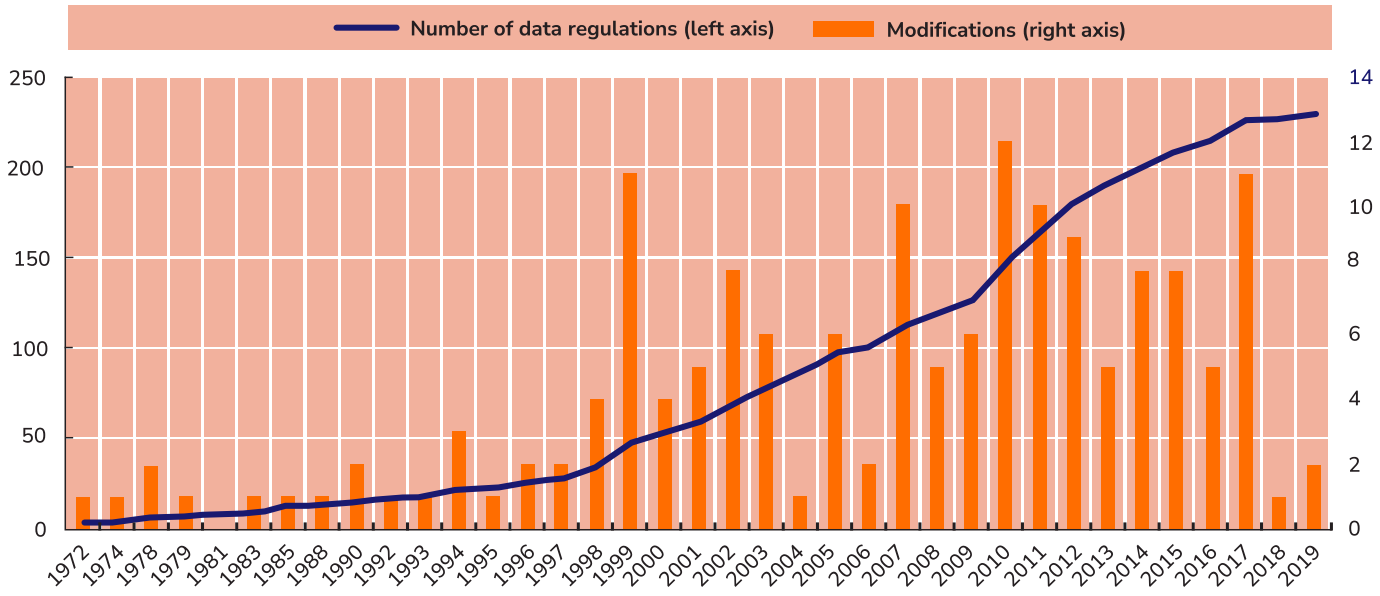
Figure 4: Data protection and privacy legislation worldwide



Harmonisation between national regulation is structurally challenged. To begin with, national data protection legislation is not only evolving itself but increasingly intersects with sector specific law and interventions. At a minimum, this concerns digital trade agreements that explicitly grapple with cross-border differences in access, protection and privacy law and enforcement. Simply taking stock of differences in principles and divergence of rules is complicated enough. Legislation is rarely codified in a manner that facilitates the job of harmonisation or cross border compliance; it is difficult to even systematically identify gaps in between different jurisdictions' rules. With the advent of machine-led data processing and compliance, codified and machine-readable legislation will become a prerequisite for efficient cross-border data management. It is also worth recalling that even if laws are in some cases tightly aligned (think, for instance, of the EU), the results of enforcement may differ by jurisdiction due to the legal system and context of other national laws and institutions in which they are applied.

Markets have already fragmented in ways that make harmonisation or reconciliation difficult. This impacts inherently scalable cross-border business models and operations most. At the risk of over-simplification, regulatory approaches to data have largely split into market, rights and state led approaches. In the US, the market has been given relatively free range to shape the way data is handled. Of late, anti-trust authorities have begun to intervene to curtail concentrated market powers, but the ultimate impact such measures will have is not yet clear. In Europe, an underlying driving force behind not only GDPR, but also the recent legislation on data, data governance and digital markets is the imposition of (consumer) rights and protections. In China, legislation and other forms of state intervention have substantially modified a landscape that was initially being driven by the behaviour of large-scale superapp platforms. Even if we acknowledge important nuances that these descriptions overlook, the challenge of reconciling the approaches in these jurisdictions to ease cross-border data flow is evident.

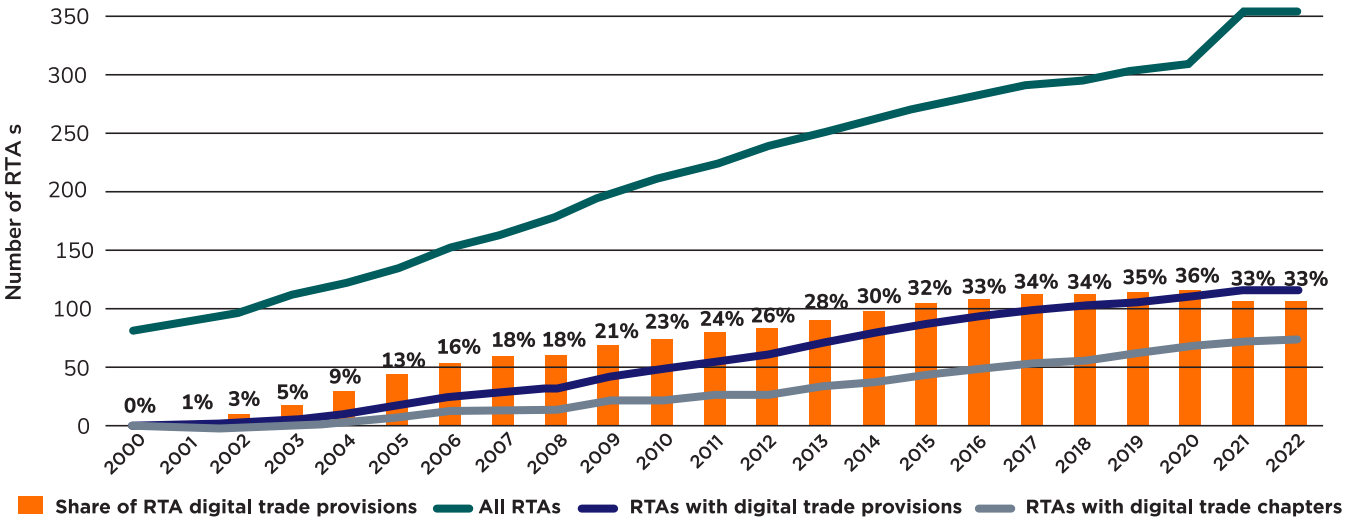
Figure 5: Growing number of regulations affect cross-border data flows



Source: Casalini and López González (2019[16]).

Digital trade agreements introduce another set of policies that impact cross-border data regulation. Digital trade provisions are becoming ever more commonplace as countries seek to adjust their policies to both promote and protect the digital economy. Their role is generally to remove barriers to cross-border data flow and usage, to facilitate digital innovation and growth. Such elements of policy can include measures to establish equivalence between data protection and privacy regimes. Often, they pertain to regulations covering e-commerce, data processing industries and measures to enhance cross-border access to controlled data sources such as credit bureaus or corporate registers. Alignment of trade agreements with data privacy and protection measures present additional challenges for policy design.

Figure 6: Regional Trade Agreements with digital trade provisions



Source: Lópex-Gonzalez, Sorescu and Kaynak (2023).

Note: The analysis only considers agreements notified to the WTO and currently in force. RTAs with digital trade provisions are defined asagreements with at least one e-commerce/digital trade provision. Digital provisions are identified from the Trade Agreements Provisions on Electronic-commerce and Data (TAPED) database (accessed August 2022 (Burri, Vasquez Callo-Müller and Kugler, 2022)

The Potential of New Technologies, Infrastructure & Ecosystems

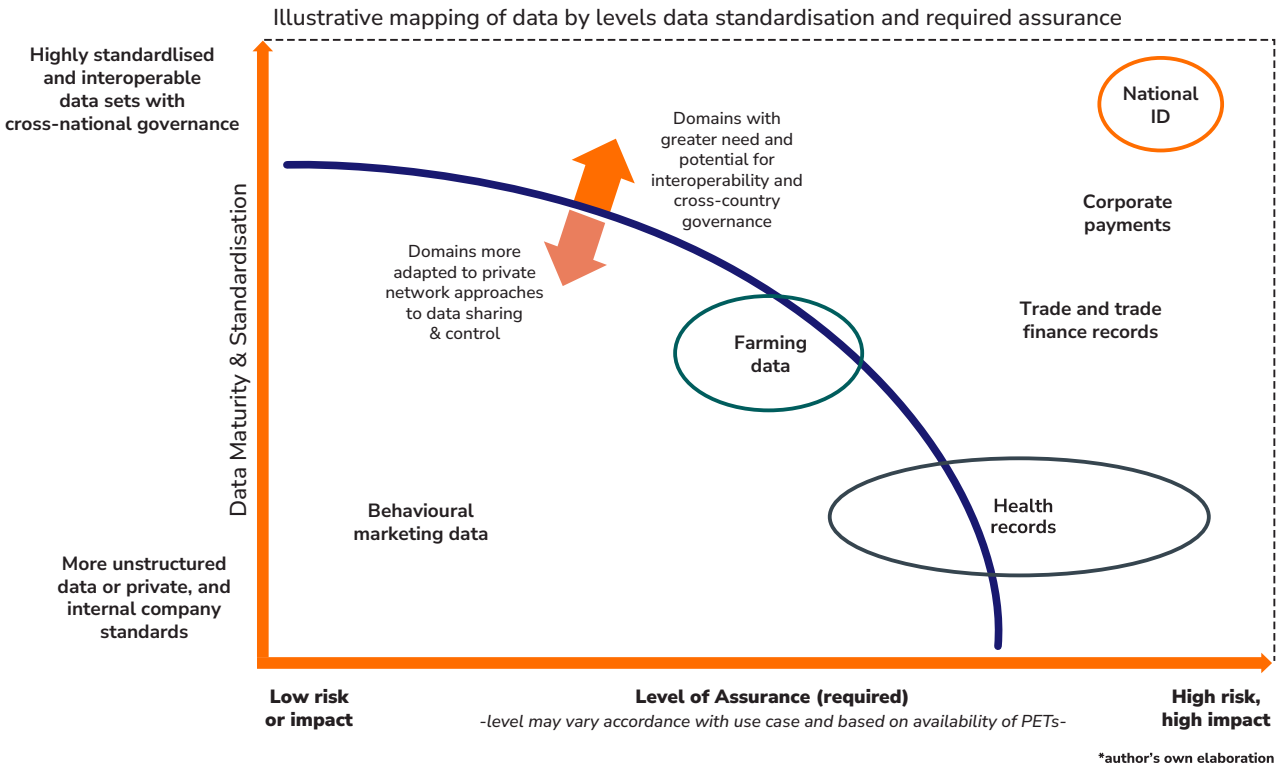
Solutions may lie in arrangements that accord data subjects greater legal and operational control and autonomy over their data. More granular control over access to data and to whom and for what purpose it is assigned will require more user education and capacity, but could alleviate issues posed by centralised control and prescriptive regulation. Data ecosystems are increasingly building upon a new array of data intermediaries, distributed ledger ecosystems and off-chain data repositories, accessible to Privacy Enhancing Technologies (PETs). These types of innovations present alternatives to one-size fits all frameworks and could enable varying levels of assurance as data is shaped, analysed, shared and managed beyond the boundaries of legacy institutions and corporate silos. New legislation in some markets is taking a positive step by strengthening data subjects' (primarily consumers') rights to access, control, and use their own data. These laws often emphasise interoperable standards, making it easier for individuals to move their data between different platforms. The orchestration of technologies, business models and regulation into effective solutions requires further experimentation and coordination.

New methods of verifying identities are emerging, which can be crucial for building trust in open or permissioned decentralised data ecosystems. These ecosystems allow data to be shared and used without relying on a single central authority. Private and public digital identity schemes and wallets may provide a new array of trusted credentials for individuals; in the corporate world, national and international identity and verification services are emerging. This includes GLEIF's recently launched verifiable credential version of the Legal Entity Identifier (vLEI). This will help counterparts verify the roles and authenticity of signatories, data and credentials across decentralised data sharing networks using a common trusted identifier. Other initiatives are grappling with the need for further elements of the economy - including fields[5] and farmers - to have trusted but interoperable identities to which to map data attributes and provenance.

Data standards initiatives will facilitate new data sharing schemes. The growth of digital business models and opening up of closed networks is driving market participants to forge common standards that facilitate interoperability. Data sharing scheme are emerging in closed corporate networks where assurance and standards can be controlled; in areas that cross industry and corporate boundaries, greater coordination, sometimes under-pinned by governments, may be required to develop common standards as well as to provider for higher levels of assurance.

[5]See for instance Varda https://www.varda.ag

Figure 7: Illustrative mapping of data domains



Private law solutions may need to complement national legislation. In practice, current data sharing arrangements already rely heavily on bilateral agreements with tag-along consequences for data users to police business partners' usage of data or its derivatives, both for commercial and compliance reasons. Beyond the domain of open banking and finance, in which regulators have been key catalysts for data sharing schemes in this highly standardised part of the economy, cross-industry or value chain initiatives appear to be limited but still necessary. Large scale efforts in trade finance, such as the Digital Standards Initiative of the International Chamber of Commerce, are progressing. But these initiatives still need to be anchored in national and cross-jurisdictional legal frameworks, such as the Model Law on Electronic Transferable Records (MLETR) by UNCITRAL.

Recommendations & Considerations

The JFF dialogue introduced several ideas and considerations about how to enhance data free flow while addressing other policy concerns and objectives that pertain to data, consumer protection and the digital economy. This section outlines points for further discussion.

- **Expand public-private and cross-sectoral dialogue**

  Policymakers and industry stakeholders are in favour of enhanced and structured dialogue to inform the evolution of data policies. Arrangements should bring together stakeholders from different sectors and government departments, recognising the varying sector issues, levels of standardisation, assurance and economic drivers for data sharing. They need to address not a one-off process of law making but deal with a longer term process in which the market circumstances, standards, risks and tools available will evolve and impact the scope and approach for regulatory alignment. The variety of data, sources and usage can be expected to expand alongside the services for processing and analysis. Meanwhile, it is likely that the attitude of consumers, data subjects and other users towards privacy and their awareness of risks will evolve in parallel. Uptake of sophisticated business models, such as artificial intelligence, are also changing the scale, risks and types of market participants involved in data sharing ecosystems. Ongoing, structured monitoring, dialogue and exchange will need to anticipate this evolving landscape to keep parties up to date on the changing context, foster mutual understanding among decision makers and provide input to different levels of national, international and domain-specific regulation and interventions.

- **Harness practical, applied testing and development ecosystems**

  Dialogue should be complemented by practical co-developments and test-and-learn experimentation. Policymakers need to be able to observe and react to the same market developments and practices to transpose principles into practical measures. The complexity, diversity and opaque nature of many developments in data makes it essential for regulators to be able to also experiment with industry members, not just to enhance their understanding, but also devise and adapt practical instruments and market regulation to achieve policy aims. For instance, the development of Privacy Enhancing Technologies (PETs) — for enhancing control, reducing data exposure or harnessing market incentives — may benefit from hands-on interactive ecosystems that enable policymakers and firms to engage in joint innovation. Experience from initiatives such as the BIS Innovation Hubs or regulatory sandboxes could provide input for similar cross-jurisdictional and sectoral arrangements for data policy.

- **Transition to codified and machine-readable legislation and regulation**

  Cross-border harmonisation of data regulation requires policymakers to have a clear, operational understanding of differences between jurisdictions. Faced with a rapidly evolving and diverse landscape of policy aims, even this first step of having clarity on the differences is challenging. That makes it problematic not only for policymakers to agree (and to agree to disagree on some elements) but it suggests how difficult it is

for industry participants to comply with a complex web of regulations in a cross-border context. Moreover, the problem will get worse as more and more data sourcing, processing and analysis will be driven by machines and algorithmic functions. The task of compliance will become impossible for humans to fulfil and require regulation itself to increasingly be codified, granular and machine readable in ways that are compatible across jurisdictions. Policymakers need to address this foundational issue to the way they operate.

- **Integrate data policy within Digital Public Infrastructure interventions**

  Practical policy and regulatory instruments to enhance cross-border data should work with initiatives in Digital public Infrastructure (DPI). The G20 recently declared its support for the role that Digital Public Infrastructure can play in development. It emphasised the need for basic functions that enable participation in the digital economy, notably, abilities to identify and authenticate individuals and businesses, and secure the seamless flow of money and information. While countries have divergent approaches and priorities, many are taking steps through public and private market interventions to build out layers of underlying infrastructure that can underpin more secure, trusted and equitable data flows between jurisdictions. The governance and architecture of infrastructures for identity, payments and data will directly impact the cross-border landscape for data regulation and compliance. These domains of government and industry intervention must be coordinated.

- **Strengthen policy engagement with data intermediaries**

  Data ecosystems will increasingly depend on and in turn shape the roles of a diverse array of data intermediaries. Business models and regulation of data intermediaries are still in flux. They range from the role of existing big tech platforms to so-called independent data wallet providers. They will include a growing array of intermediaries, consent manager and analytics providers. How they operate will also impact the risks associated with data transfers and how liability among participants is allocated and managed. Policymakers need to enhance engagement with actors in this diverse landscape, to better understand the emerging market structures and their interdependencies with regulation. Policy frameworks need to anticipate changes, accommodate different market structures and allow diverse intermediary models to coexist in the same jurisdiction, to support cross-border data ecosystems.

- **Embrace decentralisation and support new public goods it requires**

  Digital data ecosystems are inherently 'border agnostic'. Data protection and privacy laws, on the other hand, follow the contours of national jurisdictions and the myriad centralised and federated structures. Decentralised structures are more open to inclusive and rapid scaling of data sharing. Beyond high profile blockchain initiatives, there is a wider array of structures and institutions that can help to enhance data free flow but which require a new — or at least modernised — set of public goods, backed by governance and institutions that strengthen trust and control. This will include decentralised identifiers such as the vLEI, protocols, data standards and scheme managers that set and have capacity to enforce compliance with transparent rules and principles of data management access and control.

[6]See OECD 2020 paper on Shaping the Future of Regulators

- **Strengthen cross-sectoral cooperation**

  Data defies and indeed has its greatest value when it can traverse traditional industry boundaries. Regulations and authorities bound to specific industries will continue to face challenges to their effectiveness if they do not directly address the complexity and fluidity of data ecosystems. While we cannot be expected to reinvent the boundaries of existing authorities, the digital economy more generally challenges economic regulation by blurring the traditional definition of markets[6]. Data policy and regulation will need to proactively acknowledge this structural trend and explicitly seek out pragmatic ways to address it, at the least through enhanced cross-sectoral cooperation.

- **Enhance focus on the potential role of new technologies and data architectures**

  Policymakers should strengthen engagement with and support for innovations that could help enhance data free flow while addressing the industry and policy aims. Many industry participants and observers see potential in combining decentralised ledgers, off-chain data storage and consent-based data sharing. Advances in PETs, the use of personal (and organisational) data servers, and the use of semi-fungible tokens to digitise trust could help to enhance data sharing while enabling better control, monetisation, monitoring, and privacy. But the potential of these approaches may be dependent on forging new market and ecosystem structures. These are unlikely to emerge autonomously, i.e. without some form of public sector intervention. Actions are required at a domestic level but with a driving force to promote coordination at an international level aligned with the 'border agnostic' contours of the digital economy and new business models.

References

Centre for Strategic & International Studies. Operationalizing Data Free Flow with Trust. https://www.csis.org/analysis/operationalizing-data-free-flow-trust-dfft

Diane Coyle and Annabel Manley. "What is the Value of Data? A review of empirical methods". Bennet Institute for Public Policy. 2022. https://www.bennettinstitute.cam.ac.uk/wp-content/uploads/2022/07/policy-brief_what-is-the-value-of-data.pdf

G20 New Delhi Leaders' Declaration. https://www.mea.gov.in/Images/CPV/G20-New-Delhi-Leaders-Declaration.pdf

Heidebrecht, Sebastian. "From Market Liberalism to Public Intervention: Digital Sovereignty and Changing European Union Digital Single Market Governance." Journal of Common Market Studies Vol 62 Number 1, 2024.

OECD. Key issues in Digital Trade. OECD Global Forum on Trade 2023 "Making Digital Trade Work for All". October 2023. https://www.oecd.org/trade/OECD-key-issues-in-digital-trade.pdf

Moving Forward On Data Free Flow With Trust - New Evidence And Analysis Of Business Experiences. https://www.oecd.org/sti/moving-forward-on-data-free-flow-with-trust-1afab147-en.htm

Shaping the Future of Regulators: The Impact of Emerging Technologies on Economic Regulators. 2020, OECD https://www.oecd.org/gov/regulatory-policy/shaping-the-future-of-regulators-db481aa3-en.htm

UNCTAD. Data Protection and Privacy Legislation Worldwide. https://unctad.org/page/data-protection-and-privacy-legislation-worldwide

WTO. Digital Trade for Development. 2023 https://www.wto.org/english/res_e/booksp_e/dtd2023_e.pdf