OECD publishing

Please cite this paper as:

Casalini, F. and J. López González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, No. 220, OECD Publishing, Paris.
http://dx.doi.org/10.1787/b2023a47-en

OECD Trade Policy Papers No. 220

Trade and Cross-Border Data Flows

Francesca Casalini, Javier López González

JEL Classification: F13, O3

OECD TRADE POLICY PAPERS

The publication of this paper has been authorised by Ken Ash, Director of the Trade and Agriculture Directorate.

This document has been declassified on the responsibility of the Working Party of the Trade Committee under the OECD reference number TAD/TC/WP(2018)19/FINAL.

Comments are welcome and should be sent to tad.contact@oecd.org.

TRADE AND CROSS-BORDER DATA FLOWS

Francesca Casalini and Javier López-González (OECD)

The ubiquitous exchange of data across borders has given rise to a range of concerns by governments and citizens about some of the effects of so much information being collected and used, often without the knowledge of data subjects. This has led countries to condition or prohibit the transfer of data abroad, affecting trade in the process. This paper develops an indicative taxonomy of domestic approaches to cross-border data flow regulation and local storage requirements; it then surveys international instruments that address the question of international data transfers. The paper then examines the issues that data flow restrictions might raise for consumers and businesses. Against this backdrop, the paper highlights the challenge of finding balance between ensuring that important objectives, such as consumer privacy and security, are met while maintaining the benefits from free flows of data, including the benefits from increased and more inclusive digital trade.

Key words: Digital economy; data-flows; privacy; trade policy

JEL codes: F13, O3

Acknowledgements

The authors are grateful to Adrien Sene for his excellent research assistance and to Julia Nielson for her guidance, advice and support. We would also like to thank Anne Carblanc, Michael Donohue, Janos Ferencz, Marie-Agnes Jouanjean, Evdokia Moïsé, Elettra Ronchi, Vincenzo Spiezia, and Jan Tscheke for their useful comments. Valuable feedback and direction in developing and finalising this study were received from the OECD Working Party of the Trade Committee. Finally, the authors would like to thank Jacqueline Maher and Michèle Patterson for preparing this document for publication.

Table of contents

Figures

Boxes

Executive summary

This paper provides an overview of different approaches to cross-border data flow regulation with a view to helping trade policy-makers better understand the emerging landscape. The paper takes a trade perspective, focusing on the cross-border elements of data regulation most likely to impact international trade. This is without prejudice to the objectives of data regulation, the means by which these objectives are achieved, and debate on the role of trade negotiations.

There are many reasons why countries may wish to regulate data flows. One is to safeguard the privacy of individuals and their personal data. The approach to privacy and personal data protection varies across cultures, which is why regulation also differs. Countries may also restrict the flow of data, or mandate that data be stored locally, in order to meet other regulatory objectives such as access to information for audit purposes. Restrictions to data flows might also arise for the protection of information deemed to be sensitive from a national security perspective, or to enable national security services to access and review data. Lastly, some countries are also increasingly using data regulation with a view to helping develop domestic capacity in digitally intensive sectors, as a form of digital industrial policy.

Against this backdrop, there can be said to be four broad approaches emerging to the regulation of cross-border data flows. At one extreme, there is the absence of cross-border data flow regulation, usually because there is no data protection legislation at all (largely in least developed countries). While this implies no restrictions on the movement of data, the absence of regulation might affect the willingness of others to send data.

The second type of approach does not prohibit the cross-border transfer of data nor does it require any specific conditions to be fulfilled in order to move data across borders, but it provides for ex-post accountability for the data exporter if data sent abroad is misused.

A third type of approach conditions the flow of data by permitting transfers only to countries that have received an *adequacy* determination (i.e. a public or private sector finding that the standards of privacy protection in the receiving country are adequate), and/or in the event that appropriate private sector safeguards, such as contractual mechanisms, are provided, or in the case of some narrow exceptions.

The last broad type of approach relates to systems that only allow data to be transferred on a case-by-case basis subject to a review and somewhat discretionary approval by relevant authorities. This approach relates not only to personal data for privacy reasons but also to a more sweeping category of data referred to as “important data”, including in the context of national security.

Overall, there appears to be a trend towards introducing or updating data protection regimes and regulating data flows. There are many approaches of the third type, notably to respond to growing concerns over privacy, and a number adopting the fourth and second types of regulation.

Closely related to data flow restrictions are local storage requirements, or the requirement that data be stored locally. Some of these requirements are not accompanied by flow or processing restrictions and tend to be more sector-specific, targeting business accounts, telecoms or banking data and can be aimed at meeting regulatory oversight objectives or data retention policies. Other approaches combine local storage and processing

requirements and can be sector-specific or general. Finally the most restrictive approaches combine local storage with processing and flow requirements.

There are also a number of international data protection instruments that address the issue of data transfers, largely in the context of personal data: the OECD Privacy Guidelines, Convention 108 of the Council of Europe or the APEC-Cross Border Privacy Regulation System.

Increasingly, explicit provisions addressing data flows and local storage requirements are emerging in trade agreements, such as the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) and the US-Mexico-Canada Agreement (USMCA). The European Union now also proposes horizontal provisions on cross-border data flows and personal data protection in its trade agreements. However, there is no agreement on the extent to which personal data protection measures should fall under the purview of trade agreements.

Nowadays, firms of all sizes and across all sectors use data. Multinationals rely heavily on cross-border data flows for their day-to-day operations; they use data from their affiliates around the world for a large number of internal, or back office, tasks and even routine decisions. Cross-border data transfers have also enabled the creation of a new breed of micro-small and medium-sized enterprise (MSME), the "micro-multinational", which are born global and constantly connected.

It is widely acknowledged that an important factor to ensuring that the benefits of digital trade for both businesses and consumers materialise is the degree of trust in the activities of different players operating in the digital space. But with the growing collection of personal data, the risks to individual privacy increase and consumers are increasingly asking for assurances that their data is being handled appropriately. There might also be trade-offs between benefiting from highly personalised and often 'free' services and the extent to which consumers are able to keep their data private. The optimal choice in this trade-off will also vary according to individual preferences.

Firms also recognise the importance of maintaining the trust of their consumers, and privacy/personal data protection is seen as a key element in ensuring that trust. But some firms are concerned about the emerging data regulation, including in terms of the feasibility and potential cost of separating personal data from other data. Where firms are unable to separate data, a measure on cross-border transfers of personal or personally identifiable data might in effect become a measure affecting all types of data. As the digital transformation is pervasive, the issue of data flows is of interest to firms across all sectors.

In this context, the challenge is to find balance between ensuring that important objectives, such as consumer privacy and security, are met while maintaining the benefits from free flows of data, including the benefits from increased and more inclusive (e.g. of SMEs) digital trade.

Given the range of approaches and the cultural and social traditions that underpin them, one solution is to explore how existing approaches to regulating cross-border data flows can be made more interoperable —for example by drawing on the elements of convergence across international approaches.[1]

[1] In this context, the term interoperability refers to the ability of "systems, regulatory frameworks, technologies or standards to interact, communicate and function with those of other operators or countries" (Casalini et al. 2019).

While there are different views about the role of trade policy in this debate, it should be noted that trade policy will not determine the "what" of privacy protection; that is the role of regulators. While in one view issues related to interoperability in the case of privacy regulation should be the prerogative of the privacy community, another view is that trade principles – that regulations be transparent, applied in a non-discriminatory manner to countries where like conditions prevail, and are not more burdensome or trade restrictive than necessary to achieve their objective – can be helpful in informing consideration of how to move towards more interoperable approaches. Other rationales for regulating data flows – such as industrial policy or national security – also pose challenges for which international cooperation and trade principles can be helpful in ensuring that the benefits from digital trade can materialise.

1. Introduction

Today, the world is globalised and digitalised. The Internet and other information and communication technologies (ICT) are driving the development of new business models transforming how and where goods and services are produced and traded (Lopez-Gonzalez and Ferencz, 2018).[2] In this digital age, trade and production are heavily dependent on moving, storing and using digital information (data), increasingly across borders. Data enables the coordination of international production processes through global value chains (GVCs), it helps small firms reach global markets, it is an asset that can itself be traded, a conduit for delivering services and a key component for automation in trade facilitation (Lopez-Gonzalez and Jouanjean, 2017). In the digital age, data is the lifeblood of international trade.

However, the ubiquitous exchange of data across borders has given rise to concerns by governments and citizens about some of the negative side effects of so much information – in particular personal data or personally identifiable information – being collected, transferred and used, often without the knowledge of those individuals to whom the data refer. For some countries, concerns related to privacy – but also in some cases, national security – have led to growing calls for deeper and more widespread regulation of the Internet and its underlying data flows. As a result, governments are updating data-related regulations and increasingly conditioning the transfer of data across borders or requiring that data be stored locally.

Digital infrastructures such as the Internet were born global and although they offer new opportunities for people and countries around the world, they also raise considerable challenges for domestic and international policy in a world where borders and regulatory differences between countries remain. For instance, while regulations related to privacy and security are not traditionally associated with trade, they *can* have trade consequences, when, for instance, they affect the movement of data that is critical for the coordination of global value chains (GVCs) or for an SME to trade.

To support dialogue in this area, this paper aims to unpack some of the underlying issues at stake in this debate. It takes a trade perspective, focusing on the cross-border elements of data regulation most likely to impact international trade. This is without prejudice to the objectives of data regulation and the means by which these objectives are achieved, and debate on the role of trade negotiations.

Against this background, the next section discusses what data is, how it flows and the issues it raises from a trade perspective. Section 3 provides an overview of the different approaches to cross-border data regulation around the globe. Section 4 then highlights some of the issues that data flows raise for consumers and the business community, the latter with a specific focus on manufacturing activities. The last section offers some suggestions on approaches to data flow discussions in the context of the issues arising for trade.

[2] Indeed, ICT technologies have been credited as one of the driving forces behind the recent surge in global value chain (GVC) activity (Baldwin, 2016) and SME participation in global trade (Meltzer, 2014).

2. Data, data regulation and emerging trade concerns

The effect of the digital transformation on the conduct of everyday life and work has been nothing less than revolutionary. Digitalisation has permeated every aspect of economic activity and its influence is only expected to continue to expand and accelerate. It has given rise to new "information industries" such as cloud computing or big data analytics which are now making significant contributions to GDP (OECD, 2017a). The use of data has also transformed manufacturing, fostering a new production revolution (OECD, 2017b), and changed how we grow and distribute food (Jouanjean, 2019).

This digital transformation has resulted in an unprecedented increase in the flow of data both within and between countries. Estimates for global bandwidth use show an annual compound growth rate of approximately 40% between 2009 and 2013 (TeleGeography, 2015) with recent studies suggesting that data transfers were 45 times larger in 2014 than in 2005. This translates into an estimated contribution of USD 2.8 trillion to global economic activity, or 3.5% of global GDP (MGI, 2016). The pace of change shows no signs of slowing down – the size of the Internet economy is expected to more than double for G20 economies, with even faster growth rates for developing economies (BCG, 2012).

As data becomes increasingly critical to economic activity and trade, understanding what it is, how it flows and how value can be derived from its use becomes ever more urgent.

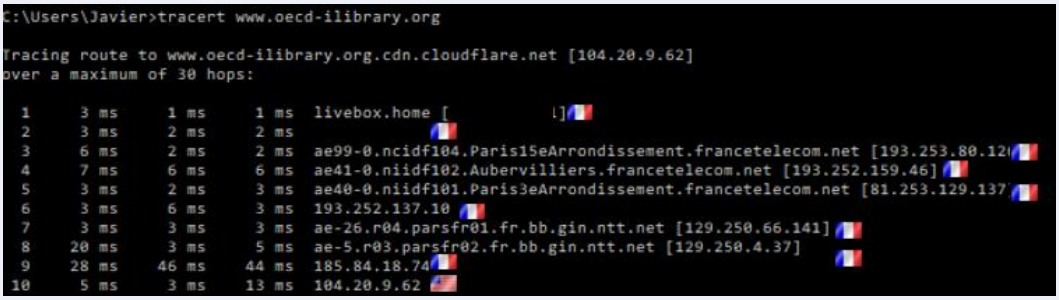
2.1. What is data and how do data transfers take place?

In structure, the Internet is a "network of networks", and, as such, it is reliant on the ability to transfer data across networks (Mandel, 2014). Data sent through the Internet travels in "packets", crossing different countries to reach its destination, making it difficult to identify, *a priori*, the geography of a data flow. The task is further complicated because firms tend to use "mirrors", located in different countries, to replicate webpages to increase the speed and reliability of data transfers (Box 1).

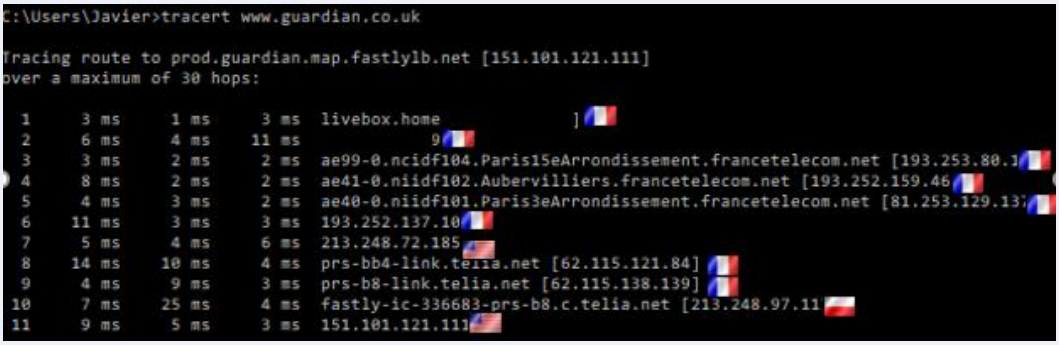
Box 1. How data travels through the Internet

The internet is a global network of computers, each with its own *Internet Protocol* (IP) *address* (an identifier of a device on the Internet). When a file is sent from a computer in Country A to a recipient in Country B it is first broken down into different '*packets'*. These are like little parcels of information marked with the IP address of the sender, that of the recipient and a code identifying the sequence in which the packets are to be reassembled at destination. Once the packets are ready, they leave the origin computer, crossing different networks and taking different routes to destination. *Routers*, the traffic wardens of the Internet, guide the packets across networks, ensuring that, at each step, they take the shortest or least congested route. Once the packets arrive at destination, the computer assembles these according to their pre-specified sequence. If a packet is missing, a signal is sent for that packet to be re-sent.

A priori, the routes of packets cannot be easily determined, but a posteriori, the path they take to a particular internet destination can be traced (e.g. using the "tracert" command in the command prompt) revealing what might be considered as "irregular" travel patterns. For example, when accessing the OECD library from a computer in Paris, packets query a server in the United States (figure below), showing how what might be considered as a purely domestic information request is in fact a cross-border one.



In addition, when accessing a British newspaper from Paris, the packets take a route that involves three countries – France, the United States and Poland, but not the United Kingdom (see below).



A few important characteristics of cross-border data flows are worth highlighting.

- Packets take different routes when flowing between two countries, often crossing different third countries.
- The ultimate origin and destination of data flows is often a technical issue. For example, firms use mirror sites which replicate webpages in different countries to increase the speed of data transfers.
- In some instances, what might seem to be a domestic transfer involves a cross-border flow.

Today, data transfers "occur as part of a networked series of processes made to deliver a business result" (Schwartz, 2009), but how this translates into 'dollars and cents' is hard to calculate. Data has no or little intrinsic value (Box 2). It is how data is applied or used that generates value to individuals, businesses and the economy.

Indeed, data is to be valued at use rather than by volume.[3] For instance, an excel file with 100 personal shopping entries may occupy the same memory space as one with 100 personal health records but its underlying value is very different depending on the perspective of the final user: whether a retailer or a health service provider. Moreover, certain types of files are "heavier" than others, with recent estimates suggesting that, by 2021, 82% of internet traffic will involve video (Cisco, 2017).The value of data can also increase when merged to become greater than the sum of its parts. For instance, the shopping entries linked to the health records can help target advertisements towards the

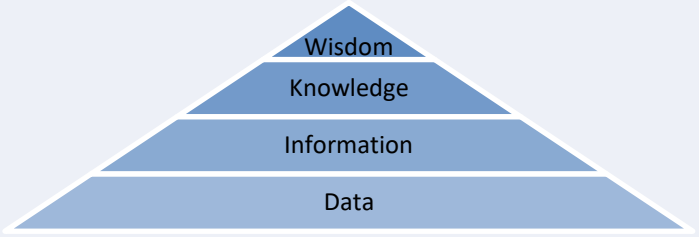
[3] See Reimsbach-Kounatze (2015) for an exploratory discussion of the implication of big data for statistics and analytics.

health conscious shopper. Data also has both inherent and potential value, meaning that information not used today can become valuable tomorrow with changing business dynamics or combined with different data yet to become available.[4]

Although data is often described as the "new oil" (The Economist, 2017), this characterisation is misleading (Mandel, 2017). Like oil, it is an essential input into the economy, however data is not scarce, and the consumption of data by one person (or company) does not prevent its consumption by others since data can be copied and transferred at virtually no cost – in sum, data is different.[5]

Box 2. Data-information-knowledge-wisdom hierarchy

Data are vast and unordered or unprocessed points that are collected; they become *information* when analysed to identify relationships between data points.[1] *Knowledge* is generated by analysts that recognise the importance of the information and *wisdom* is generated by the decisions that make the most of the streams of analysed data. In this data-information-knowledge-wisdom (DIKW) hierarchy (Figure 1),[2] each stage is dependent on those that come before it. There is no wisdom without knowledge, no knowledge without information, and no information without data.



1. Although, as highlighted in the figure, there is a difference between data and information, the paper uses these terms interchangeably.
2. This is a widely-used model within the information and knowledge management literature (Rowley, 2007).

2.2. Why is data regulation emerging?

With the ever more central role and value of data in our economy and society, the implications of data processing and data sharing touch on a large number of policy interests. For the purposes of international trade, measures that affect the possibility of exchanging and moving data across borders are particularly relevant. These measures come in the form of conditional cross-border data transfers, and/or local storage requirements.

Such measures can apply to different types of data. Indeed, data comes in many shapes and forms: it can be structured or unstructured; it can be qualitative or quantitative; nominal or ordinal; discrete; continuous; categorical; and the list goes on. However, the debate about data in the trade context often revolves around the movement of three types of data: personal data or personally identifiable information (Box 3), sector specific data (including

[4] This issue has arisen for certain business models of social network platforms which often run strong deficits during early years of operation while thinking about how to best capitalise on the mass of information gathered.

[5] See Mandel (2017) for a discussion on differences between data and oil.

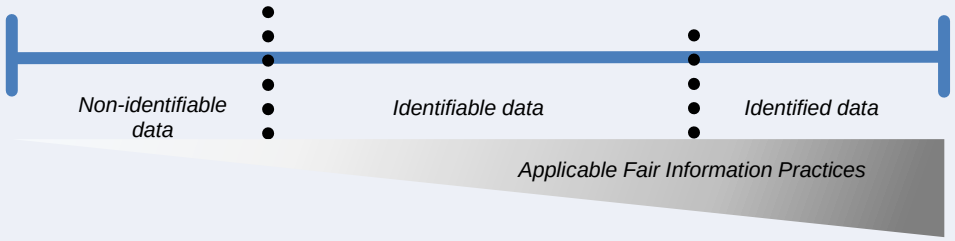
business, financial and health data), and the more recent trend towards a more sweeping and not always well-defined category of data referred to as "important" data.

Box 3. What is personal data?

Personal data or *personally identifiable information* (PII) are terms that are often used but that can mean different things to different people. Indeed, "there is no uniform definition of PII in information privacy law" (Schwartz and Solove, 2011) and conflicting definitions across jurisdictions co-exist (see National Board of Trade, 2014 and 2015). This may cause uncertainty because the presence of personal information "serves as a jurisdictional trigger" (Schwartz and Solove, 2013) to the applicability of privacy regimes.

The OECD's Privacy Guidelines (OECD, 2013) define personal data as "any information relating to an identified or identifiable individual". This implies that if one aspect of a set of data can be related to a particular individual, then the whole of that data could become personal. Moreover, with changes in technology, de-identified data might be re-identified (Schwartz and Solove, 2013), and what might be considered non-personal data today, can become personal data tomorrow.[1]

In light of these uncertainties, Schwartz and Solove (2011 and 2013) propose a non-binary definition for personally identifiable information – PII 2.0. At one extreme of the continuum there is *identified data* which relates to information that refers directly to an identified person. In the middle is *identifiable data* relating to information that brings some risk of identification. At the other extreme there is non-identifiable data which carries only a remote risk of identification (see illustrative diagram below). Schwartz and Solove (2013) argue that Fair Information Practices (FIPs) (such as limits on information use, data collection or disclosure of information; or security, transparency and data quality) should apply progressively. All should apply to identified data, but only some might apply to identifiable data and fewer still to non-identifiable data.



Differences in definitions potentially render compliance difficult for companies operating across different countries. Firms will need to assess, in an overall uncertain and often de-centralized environment, whether a particular type of data may or may not be considered personal in a given jurisdiction. In turn, this will have implications for the interoperability of different approaches to data protection, and for the free flow of data.

1. For the case of IP addresses see judgement of the European Court of Justice Case 582/14 – Patrick Breyer *vs* Germany.

The reasons why governments restrict or condition data flows, including the use of local storage requirements, can reflect a number of objectives and affect a range of data.[6]

- Much of the debate about data flows revolves around the movement of personally identifiable information (Box 3), which raises concerns about privacy. The approach to *privacy* and personal data protection varies across cultures, which is why regulation also differs.
- Some measures conditioning data flows are aimed at meeting different *regulatory objectives*, such as access to information for audit purposes. In this sense, requirements for data to be stored locally can be seen as the online equivalent of a longstanding practice in the offline world of ensuring that information is readily accessible to regulators. Such measures can be sector-specific, reflecting particular regulatory requirements and targeting specific data such as business accounts, telecoms or banking data.
- Other measures relate to *national security*, either in terms of protection of information deemed to be sensitive, or the ability of national security services to access and review data. The latter in particular can be very broad in nature, providing wide scope of access to any form of data.
- Other reasons for conditioning the flow of data or mandating that it be stored locally can be motivated by the desire to use a pool of data to encourage or help develop domestic capacity in digitally intensive sectors, a kind of *digital industrial policy*. This can reflect a view that data is a resource that needs to be made available first and foremost to national producers or suppliers. These approaches can be sector specific or apply to a range of data.

In discussing data regulation, it is important to bear in mind the underlying goals of the government. As for all policy-making, it is important to consider how effective the measures are in achieving their stated aims, the associated costs and trade-offs, and whether there are alternative measures that would enable a better balance among different aims to maximize overall benefits for the population. From a trade policy perspective, of interest is whether the same policy objective can be fulfilled in a way that has a less restrictive effect on trade.

2.3. What issues does data regulation raise for the trade community?

Nowadays, firms of all sizes and across all sectors use data (National Board of Trade, 2015), and with the adoption of new business models it is increasingly difficult for an international trade transaction to take place without a cross-border data transfer of some sort.

Cross-border data transfers have allowed consumers around the world to access a wider range of goods and services, at a lower cost. Cross-border data transfers have also enabled the creation of a new breed of MSMEs, the 'micro-multinational', which is 'born global' (MGI, 2016) and is constantly connected. Data flows allow SMEs to access IT services,

[6] While data security issues are beyond the scope of this paper, local storage requirements can be motivated by governments' belief that data stored locally might be more secure. However, the safety and security of data also depends on the quality of technical factors such as encryption and cybersecurity as well as risk management practices such as the distribution of data across different servers.

such as cloud computing, reducing the need for costly upfront investment in digital infrastructure. This allows them to be more nimble, quickly scaling-up IT functions in response to changes in demand. Better and faster access to critical knowledge and information also helps SMEs overcome informational disadvantages, notably with respect to larger firms, reducing barriers to engaging in international trade and allowing them more readily to compete with larger firms.

Multinationals also rely heavily on cross border data flows for their day-to-day operations: they use data from their affiliates around the world for a large number of internal, or back-office, tasks and even routine decisions. This includes moving human resources (HR) data to and from headquarters, sending data to R&D facilities located abroad, managing production processes and engaging in after-sale services.[7] Today, efficient supply-chain management requires the smooth flow not just of goods, services and capital, but also of ideas and managerial know-how (Baldwin, 2012).

Data is therefore a means for widening consumer choice and the affordability of goods and services, helping SMEs reach global markets and a key element of international production through GVCs. It is also a medium for the delivery of digitally enabled services across borders, and, with 3D printing, a means of delivering goods; it is an asset that can itself be traded; and an enabler of trade facilitation.

As data becomes the lifeblood of trade in the digital era, measures that affect its flow are likely to have trade consequences. In this context, trade policy makers are interested in better understanding what the consequences of emerging regulations on the movement of data might mean for trade.

3. Nature and evolution of data-related regulation

Although data-related regulation has recently received growing attention from policy makers, academics and the international press (see *The Economist*, 2017 and *The Financial Times*, 2018), it has been around for some time, dating back to the 1980s.[8] However, the growth in data-driven business models has led many countries to update their regulations, adapting them to the digital age (Figure 1).[9] It has also given rise to new regulatory approaches to cross-border elements of data regulation (examples of different approaches can be found in Boxes 4, 6 and 7).

The aim of this section is to provide an overview of different regulations that affect the movement of data across borders focusing on: i) the cross-border elements of domestic data regulation; ii) international data protection instruments; and iii) the treatment of data-flows in trade agreements.

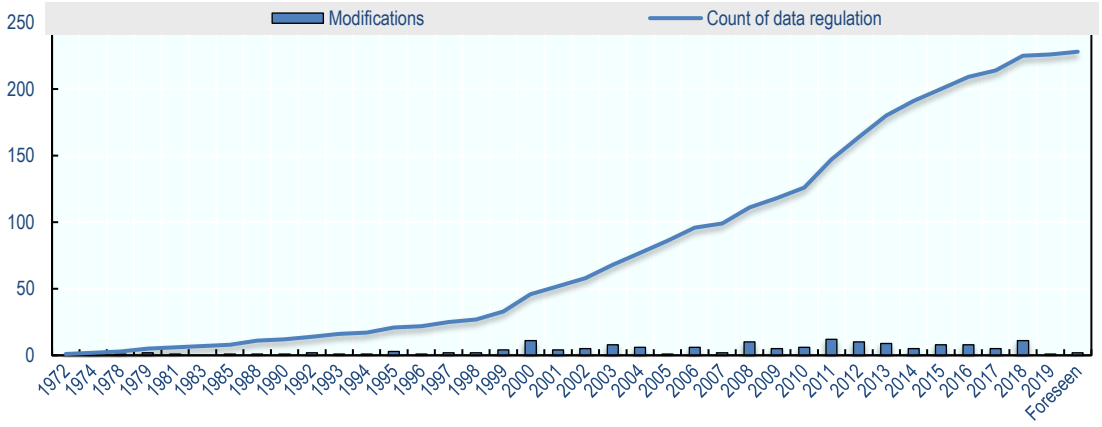
[7] See Section 4 for a more in depth discussion.

[8] Indeed, the OECD first developed its Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (Privacy Guidelines) in 1980.

[9] Indeed, the OECD updated The Privacy Guidelines in 2013 to reflect the need for greater efforts to address the global dimension of privacy through improved international co-operation and interoperability.

Figure 1. A growing number of data regulations

Cumulative number of data regulations



Note: Data protection regulations include different types of regulation relating to data transfers and local storage requirements. Numbers are affected by the way in which regulations are structured, as this varies by country; some countries may have a single regulation covering a wide range of measures; others will have several different regulations covering, for example, restrictions on data flows for different types of data, and local storage requirements.
Source: Own calculations.

Box 4. Cross-border elements of Australian Privacy Law

Australia's data privacy regulation stems from the *Privacy Act 1988* (the Act). The Act contains 13 Australian Privacy Principles (APPs) which deal with all stages of the processing of personal information, setting out standards for the collection, use, disclosure, quality and security of personal information. The Act applies to 'APP entities' including Government agencies, private sector organisations with an annual turnover of $3 million or more, and to certain smaller entities where they deal more directly with personal information (such as health care services).

APP 8 imposes strict rules on APP entities governing the cross-border disclosure of personal information held in Australia:

- APP 8 generally requires an APP entity, before disclosing personal information to a foreign recipient, to take reasonable steps (such as a contractual arrangement) to ensure that foreign recipient will handle the personal information in accordance with the APPs, and
- Section 16C of the Privacy Act makes the APP entity responsible for personal information disclosed to a foreign recipient, unless an exception applies.

There are some exceptions to APP 8 such as where a disclosure is required or authorised by law, or where other specified circumstances exist. Most relevantly, APP 8 may not apply where:

- The foreign recipient is subject to a law, or binding scheme, that has the effect of protecting the information in a way that is, overall, at least 'substantially similar' to the way in which the APPs protect the information, and
- There are mechanisms that the individual can access to take action to enforce the protection of that law or binding scheme.

An APP entity may also disclose personal information to an overseas recipient without complying with APP 8 where the entity expressly informs the individual that the principle will not apply and the individual then consents to the disclosure.

Source: Australian Government Attorney-General's Department.

3.1. Cross-border elements of domestic data regulation

Drawing on data protection legislation around the globe and on secondary sources, this section reviews *some* of the key cross-border elements of current data regulation.[10] Two types of regulations are reviewed: i) cross-border data flow restrictions (arising from data protection regulation); and ii) local storage requirements. An indicative taxonomy for each is developed below.

The manner in which countries approach their data-related policies naturally reflects the underlying preferences, including in relation to trade-offs, of their citizens. The aim of this paper is not to discuss the appropriateness of any given policy; rather, it is to document the different approaches where they relate to cross-border elements with the view to helping to clarify issues for policy makers.

Cross-border data flow regulation

Although approaches to cross-border data transfers in data protection laws differ across countries, they can be broadly grouped in an indicative taxonomy, albeit with blurred boundaries between the different categories.

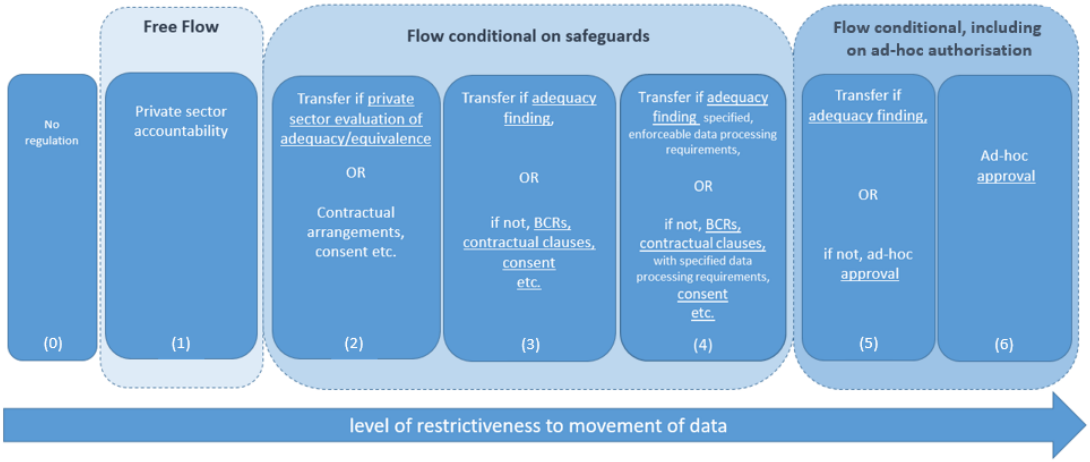
The indicative taxonomy does not aim to identify any individual country and define how it approaches the regulation of all data, as often a country may apply several different approaches to cross-border data flows depending on the nature of the data involved. For instance, there can be differences across sectors: while a country might apply a free-flow approach to movement of personal data across borders, it might condition the transfer of personal data that is health-related. Equally, a country might condition the transfer of personal data but apply a free-flow approach to all other types of data. While most of the data protection laws reviewed address the transfer of personal or personally identifiable data (Box 3), there are, however, some which refer to more sweeping categories of data, for instance, 'important data'.

An indicative taxonomy of approaches to cross border data flow regulation

The indicative taxonomy of approaches to cross-border data flows places these approaches along a continuum (Figure 2). Across these, a first distinction is made between regulations that allow for transfer of data (*free-flow*) and those that make the transfer subject to various types of safeguards (*flow conditional on safeguards*). A final category identifies flow restrictions subject to case-by-case, or *ad hoc*, authorisation (*flow conditional on ad-hoc authorisation*). Although the approaches are presented as distinct categories, the boundaries are often blurry. Moreover, how these regulations impact business activity will depend not only on the approach taken but also on the level of transparency, efficiency and non-discriminatory treatment in their application and related decision-making processes.

[10] Some of the secondary sources include: Stone et al., 2015; Kuner, 2011; USCIB, 2015; Chandler and Lê, 2014 and 2015; Ezell et al., 2013; Hufbauer et al., 2013. Other sources include privacy law publications (Norton Rose Fulbright, 2014; Hunton & Williams, 2011 and 2015; De Brauw Blackstone Westbroek, 2013), the Global Trade Alert database, national institutions and legislation databases as well as the OECDs Services Trade Restrictiveness Indicator (STRI).

Figure 2. Indicative taxonomy of approaches to cross-border data flows



Note: The elements in the figure do not singularly identify any given country's approach to data flow governance. Different approaches can apply to different types of data, even within a same jurisdiction. Note also that there are not necessarily hard boundaries between these categories of approaches. BCR stands for binding corporate rules (see Box 6 for a description).
Source: Author's compilation, based on a review of data protection legislation.

The first type of approaches, *subcategory 0*, relates to the absence of any regulation on data flows. While under this subcategory data may flow out unimpeded, concerns related to the absence of provisions on cross-border transfers, often by virtue of there being no data protection legislation, may affect the willingness of other entities or countries to send data, affecting the inflow of data from certain origins.

The second type of approaches – "free-flow", *subcategory 1*, identifies approaches that do not prohibit the cross-border transfer of data nor require any specific conditions to be fulfilled in order to move data across borders, but which provide for ex-post accountability for the data exporter if the personal data sent abroad is misused.[11]

The "flow conditional on safeguard" group of approaches includes a greater number of subcategories (*subcategories 2, 3 and 4*), all of which rely, in some form or another, on the notion of *adequacy* or *equivalence* as a condition for data to be transferred (Box 5). Within this category, each subgroup differs either in how adequacy or equivalence is applied, by whom, and the other options available for transfers in the absence of an adequacy assessment. Within this group of approaches entities operating the transfer are subject to progressively more requirements with regard to the steps that they need to take before transferring data. Hence, for entities operating in these countries greater degrees of liability exist.

[11] The term "data exporter" refers to the entity that is in control of the data and decides on its transfer abroad.

Box 5. Adequacy or equivalence

Adequacy or equivalence can either be evaluated by a data exporter or a public body. For instance, in the approaches identified in subcategory 2 (Figure 2), it is the data exporter that decides whether the recipient entity provides adequate levels of protection and conforms to applicable privacy principles.

However, and more frequently, the determination of adequacy or equivalence can be determined by a public body (such as the data protection authority, DPA), certifying that the data protection system of another country is equivalent.

This determination can take the form of a unilateral recognition, when one country certifies the adequacy of another and data can flow unimpeded in one direction. Or it can take the form of a mutual recognition of data protection measures: when two countries choose to recognise each other's systems. In this instance, once established, the free flow of data in both directions is assured (for example the recent mutual adequacy findings by the European Union and Japan).

The Privacy Shield Framework between the United States and the European Union is an example of an adequacy decision where the Commission has concluded that the European Union–United States. Privacy Shield Framework ensures an adequate level of protection for personal data transferred to Privacy Shield-certified organisations in the United States (see Decision EU 2016/1250 and Annex A for more details).

Although adequacy and equivalence are discussed here jointly, these terms do not necessarily mean the same thing. Equivalence implies the assessment of a level of objective similarity between two regulations, both in terms of the tools used and the objectives or outcomes of the regulation. Adequacy, in turn, can be more flexible as it implies agreeing on a common outcome but allowing for different tools to be used to meet this outcome.

With many approaches to cross-border data flows relying on some form of adequacy or equivalence decision, how these decisions are made is important. In line with the OECD Guiding Principles for Regulatory Quality and Performance (OECD, 2005), it is important that the regulations and related decision-making process remains transparent, non-discriminatory, efficient, in line with the stated public policy objectives and better integrate consideration of market openness principles (including avoidance of unnecessary trade restrictiveness). Today, only a few countries outline the substantive criteria used to determine adequacy in their data protection regulations.

Within this broad category, the first type of approaches, *subcategory 2*, the cross-border transfer of data is only permitted where the data exporter, on the basis of its assessment, considers that the context of the transfer ensures an equivalent or adequate level of data protection in the recipient country. However, even when adequacy or equivalence cannot be established, there are alternatives that enable transfers to take place through contractual arrangements or other fairly standard conditions such as: that the data subject's consent is obtained; that a data transfer is required to fulfil a contractual need; that a data transfer is in the public interest; that a data transfer is needed for legal cooperation; or that a data transfer is deemed necessary for the protection of the data subject's vital interests, to name the most common (in some cases, the order is reversed, with firms required to use contracts, except in cases where they assess that the other country's system provides equivalent protection).

This approach allows firms to operate flexibly but pushes them to exercise caution given that they bear the liability for the transfer. Often, although not always, in this category of approaches the regulation outlines the criteria to be used by the transferring entity in the

assessment of equivalence, inviting the firm to consider the nature of the data, the necessity of the transfer, and the applicable foreign law, among others.[12]

A further approach in the "flow conditional on safeguards" category is where the assessment of whether there is adequacy or equivalence of treatment is taken by a public body, rather than by the private sector firm, either by the Data Protection Authority (DPA) of the country or another authority in charge (*subcategory 3*). Within this category of approaches, adequacy or equivalence is established with respect to a particular country. Once a country is recognised as adequate or equivalent, data can flow freely towards that country.

This category of approaches also tends to provide options for data transfers to countries that have not been deemed to offer adequate or equivalent levels of protection. That is, transfers are still possible if at least one of a number of conditions is fulfilled, such as (pre-) approved contractual safeguards and binding corporate rules (BCR), (Box 6), or standard exceptions, as outlined earlier, apply (e.g. data subject consent, public interest, etc.). Also in this subcategory, different regulations may establish a different order of preference for different legal bases.

In sum, while a public assessment of adequacy or equivalence means that the decision is beyond the control of the potential data exporter, firms may still be able to transfer data, although this may require additional actions on the part of the firm to create a valid legal basis for the data transfer such as seeking consent, implementing precise contractual safeguards, etc.[13]

[12] Provisions falling under *subcategory 2* can read: The transfer of data abroad is only permitted where the data controller, evaluating all the circumstances surrounding the transfer, considers that the data transferred will be treated in a way comparable to that guaranteed in the domestic state. If not, the transfer can take place if reasonable steps (such as a contract) have been taken to ensure a treatment that is equivalent to that afforded by the domestic law, or if one of a list of 'standard' conditions (such as consent) is fulfilled.

[13] Provisions falling under *subcategory 3* would read: The transfer of personal data to a third country is prohibited unless the receiving country's data protection system offers an adequate level of protection. The adequacy of a country's data protection system is to be determined by the Data Protection Authority of the sending country. However, even if the recipient country does not offer an adequate level of protection, the transfer is still possible if at least one of a list of standard conditions is fulfilled (typically: model contractual clauses, consent, the need to transfer for the fulfilment of a contract, etc.).

Box 6. Binding corporate rules and standard contractual clauses

Binding corporate rules bind the affiliates of a multinational company located in different countries to apply effective rights and legal remedies for the protection of data. These rules enable data to move between affiliates located in different countries, even when these are in countries that do not recognise each other's data protection systems. Transfers are, however, restricted to affiliates within the group. While binding corporate rules provide flexibility, they are often subject to approval by the data protection authority (DPA) in the respective countries, a procedure that can be long and sometimes unpredictable in terms of outcome.

Standard contractual clauses are ready-made rules that provide for data transfers to third-parties located in other countries. The clauses, which are to be used in contracts, are developed by the DPA and, as such, are automatically considered to provide sufficient safeguards for transferring data, even to countries that do not enjoy an equivalence or adequacy recognition. While these clauses are convenient as they are ready for use, the terms they impose are relatively onerous to meet and can lead to high administrative costs.

A variant of this approach, *subcategory 4*, is as above but with added conditions relating to data processing. That is, for data to be transferred to a country that has not been granted adequacy (where data processing principles are already enforceable), the sender must fulfil the standard conditions and ensure that data, when it is processed, is treated in the same way as it would be in the sending country. Given this additional requirement, and the fact that this approach may also impose liability for the misuse of data by downstream companies on the exporting company, firms might feel comfortable with performing a transfer only where there is a prior adequacy or equivalence decision taken by the government, or where very strong contractual safeguards are in place.[14]

[14] Provisions falling under *subcategory 4* would read: The transfer of personal data to a third country is prohibited unless the receiving country's data protection system offers an adequate level of protection. The adequacy of a country's data protection system is to be determined by the data protection authority of this country. If not, the transfer is still possible if one of a list of standard conditions is fulfilled (typically: contractual safeguards (model contract clauses and binding corporate rules), consent, the need to transfer for the fulfilment of a contract, etc.) and provided that no fundamental right granted by this regulation will be at risk in the recipient country and onwards transfers.

Box 7. The European Union's General Data Protection Regulation (GDPR)

EU Regulation 2016/679 (GDPR) which builds upon the EU directive applied since 1995, entered into force on May 25th 2018. Since then, it is directly applicable in all EU member states.

The GDPR confirms and updates a number of rights for individuals with regard to their personal data. These include: the right to access their own data, the right for rectification and erasure, the right to portability (to move data), and the right not to be subject to automated decision making.

The GDPR applies to all data processing in the European Union, as well as to foreign operators if they specifically target the EU market by offering goods and services to individuals in the European Union (mere accessibility through the internet is not enough). Compared to the 1995 Directive, the GDPR expands the toolbox for sending data from the European Union to third countries, while ensuring that the protection of data is not undermined through international transfers. According to GDPR the cross-border transfer of data is possible when:

- The Commission has made an adequacy decision with regard to the data protection system of the recipient country (Box 5). These are made on the basis of a series of clear criteria such as the recipient country's rule of law, respect for fundamental rights and the applicable data protection law, among others. These criteria have been further detailed in the "Adequacy Referential" adopted by the European Data Protection Board. A recent example of such adequacy decision is the "two way" adequacy arrangement concluded with Japan.
- There are appropriate safeguards in place. These safeguard can be in the form of binding corporate rules, or standard contractual clauses (Box 6), or public agreements between enforcement authorities through codes of conduct or certification mechanisms. These need to ensure enforceable rights and effective legal remedies for individuals whose personal data is transferred;
- Statutory grounds (so-called "derogations") such as consent, performance of a contract, public interest and legitimate interests exist. These derogations should be used for specific situations and cannot be relied on for systematic transfers.

Less flexible types of approaches fall under the "flow conditional on ad-hoc authorisation" category. In the case on *subcategory 5*, the transfer depends on either an adequacy finding by the relevant public authority, or, where this is not granted, the only available option is an ad-hoc approval by the relevant authority – which does not always have to be the data protection authority.[15] Finally, *subcategory 6* does not foresee the possibility of an adequacy finding that would automatically ensure the flow of data towards a third country. It requires that *all transfers* be subject to a review by a relevant authority.[16]

[15] Provisions falling under *subcategory 5* would read: The transfer of personal data to a third country is prohibited unless: the receiving country's data protection system offers an adequate level of protection, as determined by the data protection authority; or, the transfer is authorised by the data protection authority.

[16] Provisions falling under *subcategory 6* would read: The transfer of personal data to a third country is prohibited unless the data protection authority has specifically reviewed the conditions under which the transfers take place.

Box 8. The Chinese Cyber Security Law, cross-border elements

The People's Republic of China Cyber Security Law (CSL) entered into force on June 1st, 2017. As is common in the Chinese legislative system, this is a framework law with more detailed guidelines being drafted and released subsequently. In this respect, the Draft Security Assessment Guidelines aim to bring greater clarity to the process of cross-border data transfers by supplementing the Draft Data Transfer Measures. These are yet to be finalised and other guidelines are still being drafted.

The cross-border data transfer elements of the Chinese Cyber Security Law apply to:

- Personal data, defined as information that can be used to determine the identity of natural person; and
- 'Important' or 'critical' data, defined as data related to national security, economic development and societal and public interests. This includes data in 28 sectors such as energy, manufacturing, military and nuclear.

Under the CSL two types of operators need to fulfil obligations to transfer data:

- Network operators: a broad category including owners, operators and service providers which likely refer to any company operating through a computer network (see ReedSmith, 2018); and
- Critical Information Infrastructure Operators (CIIOs), defined as those operating critical information infrastructure in important industries that may threaten the national security, national economy or people's livelihood and public interest, CIIOs are subject to more stringent requirements, including a local storage requirement.

"Pursuant to the Draft Data Transfer Measures, prior to a Cross-Border Data Transfer, an internet operator must conduct a security self-evaluation assessment (a "Self-Assessment")" (Pillar Legal, 2018). This includes specifying the purpose, type and scale of the data transfer; the countries to which the data will be transferred and the recipients thereof as well as the data safety controls taken by the operator. While a self-assessment, there is a requirement to share the report with the authorities.

However, in a broadly defined category of circumstances operators will also require a "Regulator Assessment" which will establish the legitimacy of the transfer and the risk levels associated with the transfer (categorised from low to high). Where the risk of the transfer is high, transfers shall not be allowed.

Additionally, according to the Draft Measures, an express "notice-consent" requirement in all circumstances is needed for an international transfer of personal data. Overall, the criteria that underpin the assessment or the different categories of data or of operators tend to be broad and vague, making it difficult to understand the scale and reach of the regulation.

Local storage requirements

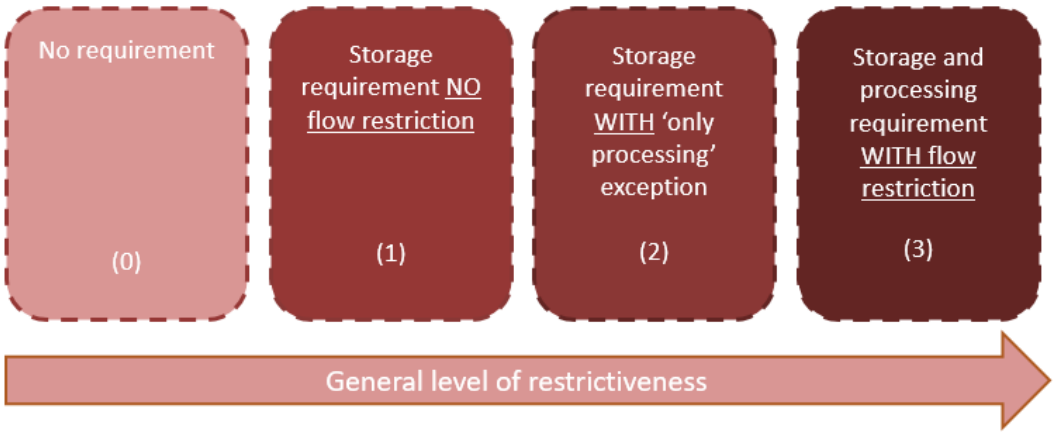
Local storage requirements constitute another type of emerging data-related regulation. As their name indicates, measures falling under this category require that certain types of data be stored in local servers, and often also include local processing requirements. Although distinct from cross-border data flow restrictions, a complete prohibition on the transfer of data amounts to a *de facto* requirement for local storage and processing. By contrast, a local storage requirement does not always correspond to a complete prohibition of cross-border transfer.

An indicative taxonomy of local storage requirements

Local storage requirements come in different forms and often target specific types of data. As with cross-border data flow regulation, even within one country different local storage and processing rules can apply to different types of data. Local storage regulations, which may or may not be accompanied by local processing requirements, can be aimed at personal data, or can be sectoral, typically targeting regulated sectors such as health, telecoms, banking or payment processing, insurance, or satellite mapping. There are also cases where local storage and processing requirements are aimed specifically at somewhat ill-defined "critical information infrastructure operators" or "network operators". Finally some approaches combine storage requirements with flow and processing restrictions.

As with regulations on cross-border data transfers, local storage requirements can be grouped under a single taxonomy identifying broad *types* of approaches, again with blurred boundaries (Figure 3). Often, local storage requirements are paired with processing and flow restrictions, where, for instance, some approaches may require that health data be stored and processed locally and that it only be allowed to move out of the country provided that certain requirements are met (see previous section). In this context, the taxonomy places the different approaches in a continuum ranging from *no requirement* to *storage and processing requirement with flow restriction.*

Figure 3. Indicative taxonomy of local storage requirements



Note: The elements in the figure do not singularly identify any given country's approach to data storage requirements. Different approaches can apply to different types of data and different types of data holders, even within a same jurisdiction.
Source: Author's compilation, based on a review of data protection legislation.

At one extreme of the taxonomy, *subcategory 0*, there is a default position where there are no requirements to store data locally. This is a relatively common category given that the number of local storage requirements remains small and targeted to specific sectors.

Next on the spectrum, *subcategory 1*, are approaches that require that a copy of the targeted data is stored in domestic computing facilities. This type of approach has no restrictions in terms of transferring or processing copies of the data abroad and its objective is, more often than not, to ensure that regulators do not encounter issues related to jurisdictional reach. Approaches falling under this category often target telecommunication metadata and business fiscal data, as a continuation of traditional data retention policies. Newer approaches to data retention now establish that data be retained and made accessible to

local authorities without prescribing the country where the data has to be stored. Data retention is also generally limited to a specified time period.[17]

Another type of approach, *subcategory 2*, relates to those where there are no flow restrictions but foreign storage is not allowed, implying that processing can occur abroad, but that post-processing, data must be returned to the home country for storage.

Progressing along the spectrum, there is a category of approaches, *subcategory 3*, that require that data be stored locally and this is combined with conditions attached to the possibility of transferring and processing those data abroad. These last two requirements can be related to a desire to encourage the development of domestic data storage and other data services industries and thus can be related to industrial policy objectives.

3.2. International personal data protection instruments

As the digitalisation of the economy has progressed, so too have the range of international instruments seeking to ensure interoperable approaches towards safeguarding privacy across national borders.

International personal data protection instruments include:

- *The OECD Privacy Guidelines* which aim to ensure the protection of privacy in the face of new challenges posed by technologies and to avoid unjustified restrictions on data flows and the economic and social benefits they enable (See Box 9).
- *Convention 108*, or *The Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, is a treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, fifty-three states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions (see Annex A for more details).
- The *APEC Cross-Border Privacy Rules (CBPR) System*, in place since 2011, is a framework developed by APEC economies to promote the interoperability of privacy regulation through enforcement of minimum standards. The CBPR System is not mandatory for APEC economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System. To date, only six of the twenty-one APEC economies are participating to the System (see Annex A for more details).

[17] In this form, these measures might be relatively innocuous. Storing data for audit purposes is something which firms have had to comply with for many years and therefore imposing a digital equivalent to this legislation should not overtly disrupt firm activity.

Box 9. The OECD Privacy Guidelines

Data flow governance has been a recurring focus of OECD work for over 30 years. Work in the 1970s led to the OECD's 1980 Guidelines on "The Protection of Privacy and Transborder Flows of Personal Data", the title of which highlights the OECD's dual concern to both ensure the protection of privacy in the face of new challenges posed by technologies and to avoid unjustified restrictions on data flows and the economic and social benefits they enable.

The Guidelines are designed to be technologically neutral and are nonbinding. The 2013 revisions to the *OECD Privacy Guidelines* (OECD, 2013b) included important updates to the data flow governance provisions. With regard to free flow and legitimate restrictions, key principles are summarised in paragraphs 16 to 19 reproduced below:

> (16). A data controller remains accountable for personal data under its control without regard to the location of the data.
>
> (17). A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these *Guidelines*.
>
> (18). Any restrictions to trans-border flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

The *Guidelines* also encourage states to cooperate on privacy matters and support the development of international arrangements that promote interoperability among privacy frameworks.

3.3. Data flows and trade agreements

There are also relevant provisions related to data in trade rules, including at the World Trade Organisation (WTO) and regional trade agreements (RTAs). While there is to date no agreed position among WTO Members on the applicability of WTO provisions, the next section presents some illustrative argumentation.

WTO rules and data[18]

Both the General Agreement on Trade in Services (GATS) and the General Agreement on Tariffs and Trade (GATT) have bearing on data flows since data measures may impact goods, goods with embodied or embedded services and digitally enabled services (see Lopez-Gonzalez and Ferencz, 2018).[19] Commitments and obligations differ under each agreement and thus assessing the legality of a specific measure is complex. For instance, under GATT rules, national treatment is automatically extended while in the GATS, national treatment is a negotiated commitment which differs across country and sector. The legality of a data localisation policy might therefore turn on the sectoral classification of the affected product.

Some of the regulatory uncertainties that data regulation raises can be illustrated using a hypothetical example of fitness trackers (taken from Chander, 2015). These are physical

[18] This section benefitted from contributions from Magnus Rentzhog.

[19] In addition, the Technical Barriers to Trade agreement (TBT) would also be relevant, especially when it comes to issues like the inter-operability of standards (Meltzer, 2015). The Agreement on Trade-Related Aspects of Intellectual Property Rights (TRIPS) might also have bearing.

products that collect fitness and health information about the user and store that data on the producer's servers. Trackers sold in one country can either be produced by a local company, or a foreign established company. The data from the local company's tracker is transferred to local servers while the foreign company's data is transferred abroad for processing. A barrier to cross-border health data flows would render the foreign fitness tracker less competitive while a ban on transfers would effectively prohibit the foreign fitness tracker unless it locates servers locally and undertakes related data processing locally.

In this instance, if considered under the GATT, the legality of the data measure will depend on whether there is an alternative, less trade distorting, policy available to the local government, while under the GATS the outcome will depend on what GATS commitments have been made by the country, and only if so, would the question of a less trade distorting policy come to play. Outstanding classification questions complicate this further. Does the fitness tracker fall under the health sector or does it provide computer and related services, or telecommunication services?

In the context of GATS, data localisation measures require companies to take actions relating to how they handle the data that is necessary for the supply of a particular service. As such, localisation measures will, in effect, relate to the supply of services as they bear upon conditions of competition between foreign and national suppliers.

The data localisation requirement could arguably create situations, not only *de jure* but also *de facto*, where foreign services and services suppliers are treated less favourably than domestic firms. However, the general exception clauses related to security, and public morals and privacy could negate the negotiated commitments from applying to data localisation measures. For the public morals and privacy exception to be valid, the specific regulation needs to meet a necessity test[20], part of which is a requirement to respect the objectives of non-discrimination and least trade distorting alternatives to the regulation (GATS Article XIV).

GATS' Understanding on Commitments in Financial Services and the annex on Telecommunications also deal with data transfers. The understanding states (Article 8) that *"No Member shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means, or that, subject to importation rules consistent with international agreements, prevent transfers of equipment, where such transfers of information, processing of financial information or transfers of equipment are necessary for the conduct of the ordinary business of a financial service supplier. Nothing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement."* For WTO Members that have scheduled according to the Understanding, this article might limit the possibilities of introducing cross-border data restrictions in the financial services sector. However, commitments under this agreement must be reconciled with the right of a WTO Member to, inter alia, protect personal data in accordance with the GATS Article XIV general exception, the above language of Article 8 of the Understanding on Commitments in Financial Services and the prudential exception in paragraph 2(a) of the Annex on

[20] In the case of privacy, the Article requires that measures *be "necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of the Agreement including those relating to:…(ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts".*

Financial Services. The Telecommunications Annex requires governments to ensure that telecommunications services can be used to access and transfer data across borders, but the obligations only apply when the actions of a public telecommunications operator have infringed this right and apply to the technical availability of the transmission channel rather than to the substance of the data transferred.

Data and regional trade agreements

With slow progress at the WTO on matters relating to e-commerce, issues related to cross-border data flows are increasingly featuring in regional trade agreements (RTAs). While provisions are generally in the digital trade or e-commerce chapters of the agreements, some relevant provisions might also found in the context of sectoral commitments. This section reviews a selection of agreements, with a view to identifying the relevant language used.

The Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) contains a relatively complete set of provisions on data movement.[21] In Article 14.10 "*Parties recognise that each Party may have its own regulatory requirements concerning the transfer of information by electronic means*". However, "*each party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person*". The Article also foresees measures inconsistent with this provision, but only "*to achieve legitimate public policy objective[s], provided that the measure: is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and…* [when it] *does not impose restrictions on transfers of information greater than are required to achieve the objective*". The United States-Mexico-Canada Agreement (USMCA) stipulates that "*No Party shall prohibit or restrict the cross-border transfer of information*" (Article 19.11) and applies similar provisions as above for exceptions.

The USMCA also contains references to the protection of personal information. Article 19.8 stipulates that "*The parties recognize the economic and social benefits of protecting the personal information of users of digital trade and the contributions that this makes to enhancing consumer confidence in digital trade".* It foresees that "*each Party shall adopt or maintain a legal framework that provides for the protection of personal information of the users of digital trade*". In the development of this framework, the USMCA references approaches such as the APEC Privacy Framework and the OECD Privacy Guidelines. It also pushes parties to "*recognize the importance of ensuring compliance with measures to protect personal information and ensuring that any restrictions on cross-border flows of personal information are necessary and proportionate to the risks presented*".

On local storage, Article 14.13 of the CPTPP stipulates that "*No party shall require a covered person to use or locate computing facilities in that Party's territory as a condition for conducting business in that territory*". In CPTPP, measures inconsistent with this are allowed in view of achieving legitimate public policy objectives provided they are not "*a disguised restriction on trade*" or "*impose restrictions on the use or location of computing facilities greater than are required to achieve the objective*".

The EU has adopted a new horizontal approach on cross-border data flows and personal data protection in trade agreements that it is pursuing in all its trade negotiations. This clause prohibits different forms of data localization and data storage measures. At the same

[21] With exceptions related to government procurement and the financial sector (Article 14.2).

time, the European Union considers privacy and data protection as fundamental rights, and the EU clause provides that "*each party may adopt and maintain the safeguards that it deems appropriate for the protection of personal data and privacy*". The cross-border flow of personal data is also not included in the European Union-Japan Economic Partnership Agreement signed in 2018. However, Japan and the European Union agreed to allow free flow of personal data through "mutual adequacy" of their respective data protection systems.

4. Perspectives from consumers and businesses

The benefits of digital trade for both business and consumers are contingent on the degree of trust that is placed on the activities of different players operating in the digital space. While both consumers and firms benefit from increased trade enabled by data flows, the aim of this section is to identify some of the concerns expressed by consumers and businesses with respect to cross-border data flows. From the perspective of consumers, concerns largely relate to how personal data is being used and the risks associated with misuse or theft of information. From the perspective of business, keeping data safe and enhancing trust remain top priorities, but concerns have emerged as to the impact of emerging data measures on the costs and ability to coordinate global value chains and/or engage in trade with some countries.

4.1. What are the key concerns of consumers?

The information trail left in today's economic and social interactions is richer than ever before. For example, in the past, when renting a DVD, the information collected by firms would be limited to the name and address of the user and the titles and dates of collection and returns of rented films. Now, with digital streaming services, firms can also collect additional data on: the time a particular movie was watched; whether it was finished or not; if it was watched multiple times; when it was paused; the extent to which it was enjoyed by the viewer (through ratings); and so forth. This information helps firms compile user profiles that can be used to make more targeted recommendations, improving service delivery.

Yet this example also helps illustrate some of the emerging concerns; namely that the amount of information gathered and the use made of it is not always clear to the consumer. With a growing online presence, more opportunities to record our activities arise, leading to a higher probability of revealing facets of ourselves that we may wish not to share with a company hence fuelling concerns about privacy protection. Moreover, additional concerns arise when the data gathered is monetised in another form, such as by selling it to other firms who may make use of it for marketing or other purposes.

But privacy itself is difficult to define. It means different things to different people (Solove, 2006) and the value we attach to privacy, whether as individuals or in society, can be subjective (see Box 9 and Acquisti et al., 2017). There can also be a trade-off between benefitting from highly personalised and often 'free' services and the extent to which consumers are able to keep their data private. The optimal choice in that trade-off will also vary according to individual preferences.

Box 10. The economics of privacy

The control of personal information can affect the balance of economic power among parties. For instance, a retailer holding information about an individual might be able to price discriminate, charging a higher price than s/he would otherwise. However, if the consumer has the informational advantage, s/he might be able to get a nice bargain instead. In this sense, information can be redistributive (Posner, 1981).

Consumers can benefit from sharing personal information. Whether this is reconnecting with long-lost friends using social networks, using search engines to respond to queries or accessing 'free' e-mail providers. The price of using these services is often the personal data of the individuals – generated while using the services provided. This data allows companies to predict the willingness to pay, or reservation price, of different types of consumers for different types of goods and services – information which can be monetised directly or sold to advertisers.

There are also positive spill-overs associated with sharing personal information. This is the case of online searches providing early alert of epidemics, or shared information about movie ratings or travel recommendations. Society may suffer when certain behaviours remain hidden (such as insider trading or sexual assault) but sometimes society can benefit when information is suppressed (such as juvenile records being expunged).

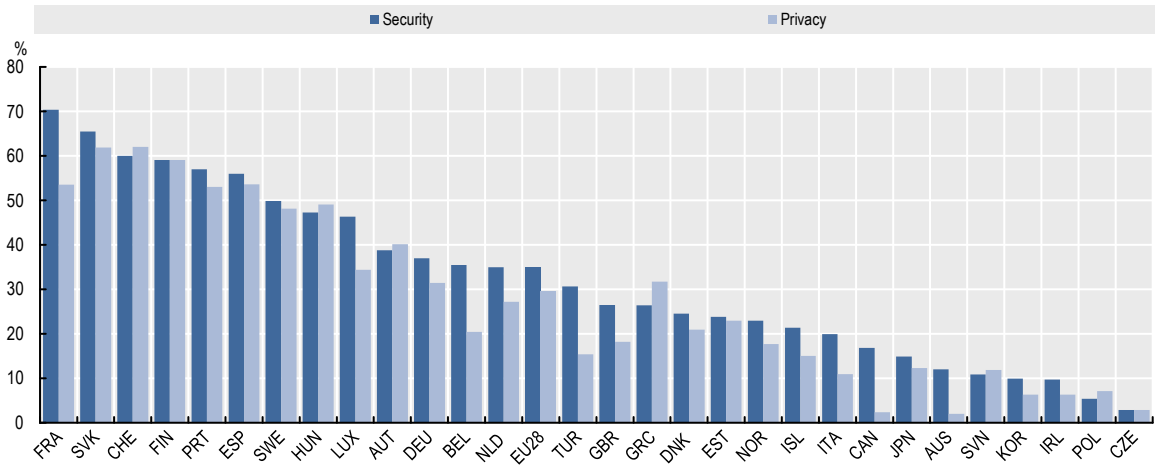
The economics of privacy is therefore not unambiguous and is wrought with trade-offs: use free online services, but at the expense of less privacy. Reveal your preferences about products so that you may find these more easily, but possibly at the expense of higher prices.

Moreover, assigning value to privacy or personal data is also difficult. Is it the price we would pay to give away our data or the amount we might pay to protect it? Is it the expected cost the data subject may suffer if her data is exposed, or the expected profit the data holder can generate from acquiring her personal information? For some, privacy is a fundamental right and thus does not have a price.

Source: Based on Acquisti et al., 2016.

However, "privacy is a critical factor that significantly influences online trust" (OECD, forthcoming). Indeed, according to OECD (2014), privacy and security concerns play a key role in determining whether consumers order online or not (Figure 4); there is thus also a strong business case for privacy protection. But with the growing collection of personal data, the risks to individual privacy increase, which is why consumers are increasingly asking for assurances that their data is being handled appropriately. Businesses increasingly see their ability to meet these demands as part of their competitive offering.

Figure 4. Percentage of individuals not ordering online because of payment security or privacy concerns (2009 or later)



Note: For Australia, data originate from the Multipurpose Household Survey as published in the Household Use of Information Technology 2012-13 and refer to 2012/2013 (fiscal year ending in June 2013) instead of 2013. "Payment security concern" relates to "concerned about providing personal details online". For Canada, data originate from the Internet Use Survey 2012. For Japan, data originate from the Internet Usage Trend Survey 2011. "Security concern" relates to "concerned about security when giving out credit card information" and "Privacy concern" relates to "protection of personal information". Data cover Internet users aged 15 and more, instead of 16-74 year-olds. For Korea, data originate from the Survey on the Internet Usage 2009 and relate to "Privacy concern" and "Security concern" as reasons for not using Internet shopping. For Switzerland, data originate from the Omnibus TIC 2010 survey.
Source: OECD, forthcoming originally from Measuring the Digital Economy: A New Perspective (2014).

4.2. How do firms use data and why are they concerned?

A number of firms have been outspoken about the negative impact that data related measures may have on their activity (see BIAC, 2016). Understanding why this is the case requires i) looking at how data supports economic activities; and ii) identifying how this matches with the nature of the emerging data measures.

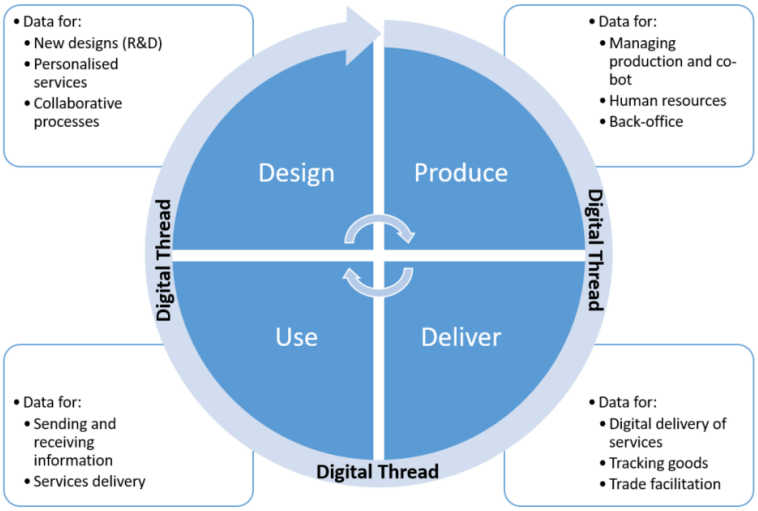
Use of data in manufacturing activities

Firms are increasingly reliant on data transfers in support of their business activities (see Box 10 and National Board of Trade, 2014 and 2015). This is not only true for firms engaged in ICT or even in services; for firms engaged in manufacturing activities, data use is pervasive in all stages of design, production, delivery and use (Figure 5).[22]

For instance, at the 'design' stage, *research and development* for manufacturing activities increasingly involves coordinating individual researchers, scientists, designers and IT specialists working in different countries and sharing ideas, information, prototypes and test data.

[22] This section draws heavily on National Board of Trade (2014 and 2015).

Figure 5. The digital thread of modern manufacturing activities



Note: The figure is schematic
Source: Author's compilation

Exercising overarching control and coordination of geographically dispersed *processes of production*, at the 'production' stage, also involves moving data across different locations: organising input flows of goods and services, working with subcontractors and suppliers, and handling internal operations. This requires, inter alia, sending data about inventories, sales, demand forecasts, order status, human resources and production schedules.

Still at the 'production' stage, as manufacturing becomes increasingly mechanised, data transfers are needed to *instruct robotics*. Sensors on the factory floor send real-time data that can then be analysed and used to make any necessary adjustment to production activities or equipment maintenance. Increasingly, this in-plant production can also require the transfer of data containing personal information of employees working alongside robots (so-called "cobot").[23]

At the 'delivery' stage, data transfers are needed to track and trace products as they are travelling to the border, across the border and beyond: data flows underpin modern trade facilitation practices. Additionally, if the product being traded is a "smart" good, the delivery of services and information, the elements that make the product 'smart', will be contingent on the ability to collect and transfer different types of data.

When the product gets to the consumer, at the 'use' stage, the experience of the consumer might also depend on the ability of the firm to receive, process and respond to continuous feedback. Increasingly, firms also offer after-sales services, the efficient provision of which requires monitoring the performance of products in view of handling maintenance, repairs, and spare parts, again all connected through data flows.

[23] Indeed, in the case of agricultural supply chains, albeit with a different motivation, firms are increasingly sharing information with consumers about the persons engaged in the process of producing and delivering agricultural products in response to consumer demand to know more about how goods are produced.

All these elements, whether at the individual stages or taken as a whole require constant digital connectivity via information and communication links supporting a 'digital thread' (Figure 5). Indeed, measures that condition access to and use of the digital thread will affect the efficacy of the individual stage and the viability of the value chain for modern manufacturing.

In contrast, local storage requirements for data may have the effect of diverting trade and production to national suppliers of intermediate goods and services much like local content requirements (Stone et al., 2015). While firms located in the domestic territory and engaged in the provision of data solutions may see their business activity increase as a result of the rise in local demand after the introduction of the measures, these gains are likely to accrue to a small segment of the firm population. Efficiency losses may arise in other firms from imposing domestic sourcing where foreign sourcing may be more cost-effective (National Board of Trade, 2015a, and Bauer et al., 2015). In this sense, a local storage requirement becomes analogous to a traditional import substitution strategy. Firms may also need to switch to potentially less reliable, less efficient and pricier local suppliers rather than accessing global digital services or international outsourcing solutions.

Firms might also have to relocate or replicate certain functions, such as after-sales services or data management facilities, to particular countries in response to the measures. This will disrupt centralised business solutions which could lead to inefficiencies arising from the loss of access to scale opportunities (denying some of the benefits of GVC participation). It could further decrease the use and efficiency of trends like 'big data' and affect the development of new ICT industries (for a wider discussion of these issues see Kuner, 2011; USITC, 2014; Kaplan and Rowshankish, 2015; Hon et al, 2015; Chander and Lê, 2014; National Board of Trade, 2014).

Box 11. Examples of use of cross-border data flows from manufacturers

Wind turbine manufacturers use data from turbines to maintain and optimise wind energy parks, often across different countries. They rely on data flows to reduce operational costs and on big data analytics to increase competitiveness by optimising wind turbine productivity and enabling the delivery of services. This requires their being able to collect, store and analyse data from different plants located across the globe.

Hearing aid manufacturers rely on the flow of data for pre- and post-purchase customisation in view of fitting devices to the ears of individual consumers. They scan the customers' ear channels so that a precise 3D-model of the inner ear can be printed. Once shipped to the customer, data flows support remote technical calibration for better delivery of hearing aid. This process involves the back and forth movement of personal, and health, data, often across borders.

An engineering equipment manufacturer and service solution provider has offices in more than 50 countries and over 12 000 employees supplying mineral and cement industries globally. The production and processing of cement plants requires the coordination of architects, engineers and entrepreneurs across different national offices which in turn entails the movement of different types of data. In terms of storage, the company has a main data centre in Denmark finding that centralisation is a cost-efficient way of organising data.

Source: Confederation of Danish Industry.

Nature of business concerns

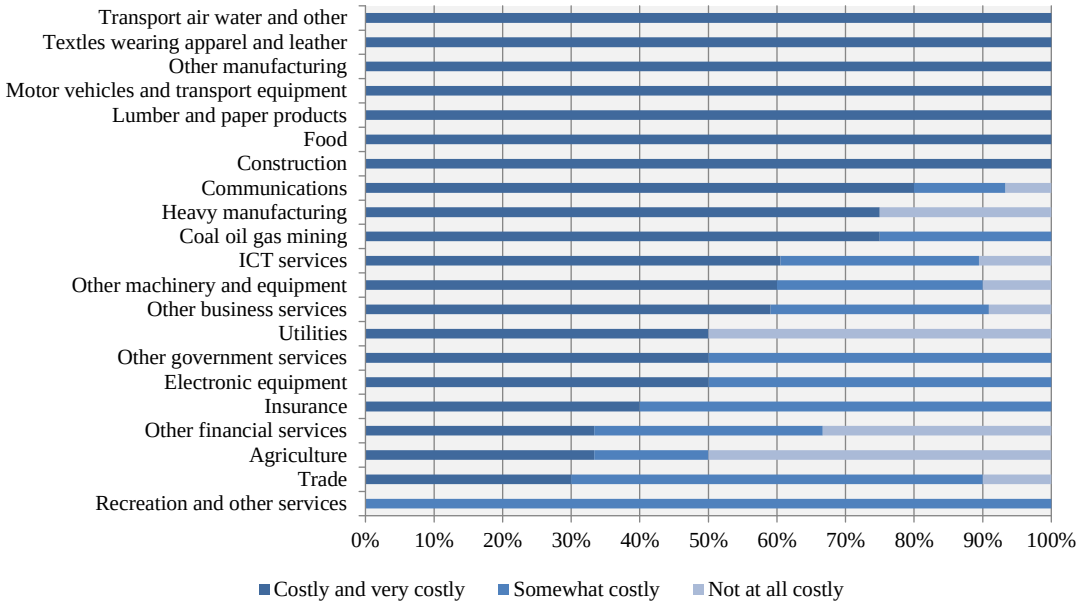
A recent business questionnaire conducted by the OECD, sought to identify some of the concerns of firms with respect to data related issues. While illustrative given the problem of achieving a representative sample on digital trade issues (given its global scale) and the normal issues of selection bias in responses, it is interesting to note several findings[24]. First, an overwhelming majority of firms, over 99% of respondents, identified privacy protection as a key element in ensuring consumer trust. Yet 78% of responding firms expressed concerns about emerging data regulation. This suggest that, despite there being a common interest in protecting the privacy of consumers, the way the emerging measures are currently tackling the issue is being questioned.

One particular concern relates to the issue of personal data. The importance of personal data varies considerably across sectors. For instance, the business questionnaire showed that, on aggregate, 50% of firms perceive that personal data represents a significant amount of the data that they handle. Although service firms in sectors such as telecommunications, ICT, financial and other business services showed the highest reliance, many manufacturing firms also reported relying on personal data (heavy and other manufacturing, machinery and equipment and to a lesser extent electronic equipment and construction). Those relying less on transfers of personal data, among respondents to the questionnaire, were firms in mining sectors, paper products, textiles and motor vehicles.

The extent to which firms can identify and split personal from non-personal data was also identified as an issue for firms. Respondents to the business questionnaire overwhelmingly reported that separating data was likely to be costly or very costly, a response consistent across most sectors (Figure 6). Where firms are unable to separate data, a measure on cross-border transfers of personal or personally identifiable data might in effect become a measure affecting all types of data.

[24] The business questionnaire, delivered online between August 2015 and March 2016 received 259 responses with firms headquartered in 48 countries and representing 21 sectors. In emerging fields of study such as this, questionnaires can be useful tools for obtaining background information to help guide research efforts. They are, however, not without caveats. For example the questionnaire can suffer from biases arising from i) the channels of distribution; ii) the modes of this distribution; and iii) self-selection. For inferences to be made about the larger population of firms an appropriate sampling strategy, ensuring the representativeness of the sample, would be needed. Obtaining such a representative sample, in this instance, would stretch beyond the resources available and therefore the results of the questionnaire are to be seen as initial information on which observations or "rebuttable presumption" for deeper analysis can be made.

Figure 6. How costly is it to separate personal from non-personal data?



Note: Bars show the share of respondents by answer given across sectors. This figure is based on answers from 165 firms. Including 18 answering "I don't know". Lumber and paper products, Motor vehicles and transport equipment, Recreation and other services, Textiles wearing apparel and leather, Transport air water and other are represented by a single firm; Electronic equipment, Food, Other government services, Utilities (2 firms); Construction (3); Coal oil gas mining and Heavy manufacturing (4); Insurance (5); Agriculture (6); Other machinery and equipment and Trade (10); Other financial services (12); Communications (15); Other business services (22) and ICT services (38).
Source: Authors' compilation from OECD Business Questionnaire.

5. Observations from the analysis

This paper has aimed to provide a broad overview of the different approaches that have been taken with respect to cross-border data regulation with a view to providing insights which might be of help to policy makers.

There are many different approaches to cross-border data flow regulation reflecting different policy objectives and cultural preferences. Overall, there appears to be a trend towards regulation of data flows, with many approaches relying on adequacy, notably to respond to growing concerns over privacy, and others having a greater focus on industrial policy objectives. Approaches relying more on private sector actions and accountabilities are also in place.

Despite these differences there may be some common threads which might suggest fruitful paths for further exploration.

- Countries are increasingly introducing personal data protection frameworks. Continued dialogue to achieve greater interoperability between these frameworks, notably in the OECD, could help provide useful guidance for the trade community. In turn, trade can help to provide the impetus and incentives for regulators to find commonalities across their different approaches, to support a global digital ecosystem.

- There are a number of countries that are using data regulation for industrial policy purposes. Bringing policies under the aegis of trade agreements to ensure that approaches remain transparent, non-discriminatory and least trade restrictive in pursuing the stated objectives might help contest these practices.
- As more countries rely on adequacy or equivalence assessments by public or private bodies, there might be scope to exchange information and views on the *processes* through which these are established.

While this paper takes a trade perspective, interoperability between different data protection systems can be important not simply for trade but, equally, for ensuring that public policy objectives such as privacy and security can be met in a global digital world.

Bibliography

Acquisti, A., Taylor, C. and L. Wagman. (2016), "The Economics of Privacy", *Journal of Economic Literature*, Vol. 52, No. 2, 2016, *Sloan Foundation Economics Research Paper* No. 2580411, March 2016.

Baldwin, R. (2012), "Trade and Industrialisation after Globalisation's Second Unbundling: How Building and Joining a Supply Chain are Different and Why it Matters," in *Globalization in an Age of Crisis: Multilateral Economic Cooperation in the Twenty-First Century*, R. Feenstra and A. Taylor (eds.), University of Chicago Press.

Baldwin, R. (2016) *The Great Convergence – Information Technology and the New Globalisation*, Bellnap Press, Cambridge (MA).

Bauer, M., H. Lee-Makiyama and E. van der Marel (2015), "Data Localisation in Russia: A Self-imposed Sanction", *ECIPE Policy Briefs*, June.

BCG, (2012) "The Internet Economy in the G-20 – The $4.2 trillion growth opportunity", accessed at http://image-src.bcg.com/Images/The_Internet_Economy_G-20_tcm9-106842.pdf

BIAC (2016), "The flow of data across borders: A BIAC trade policy perspective", [http://biac.org/wp-content/uploads/2016/03/The-Flow-of-Data-Across-Borders_A-BIAC-Trade-Policy-Perspective.pdf] accessed 22 March.

Chander, A. (2015), "Robots, the Internet of Things and the Future of Trade", mimeo, University of California, Davis School of Law, Davis CA.

Chander, A. and U.P. Lê (2014), "Breaking the Web: Data Localization vs. the Global Internet", *US Davis Legal Studies Research Paper* Series, No. 378, April 2014.

Chander, A. and U.P. Lê (2015), "Data Nationalism", *Emory Law Review*, 64, pp. 678-739.

Cisco (2017) Cisco Visual Networking Index: forecast and Methodology, 2016-2021. Accessed 18 November 2018, https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.html#_Toc484813971

De Brauw Blackstone Westbroek (2013), EU Country Guide: Data Location & Access Restriction, De Brauw Blackstone Westbroek, [available at: http://www.verwal.net/wp/wp-content/uploads/2014/03/EU-Country-Guide-Data-Location-and-Access-Restrictions.pdf] accessed on 1 December 2015.

Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-US Privacy Shield (notified under document C(2016) 4176) (Text with EEA relevance).

Ezell, S.J., R.D. Atkinson and M.A. Wein (2013), "Localization Barriers to Trade: Threat to the Global Innovation Economy", *The Information, Technology & Innovation Foundation*, Washington, DC.

Financial Times (2018) "Data Protectionism: The growing Menace to Global Trade", 13 May.

Hon, W. Kuan et al. (2015), "Policy, Legal and Regulatory Implications of a Europe-Only Cloud", *Legal Studies Research Paper* No. 191/2015? Queen Mary University of London.

Hunton & Williams (2011), "English Translation of Peru's Law for Personal Data Protection Released", Privacy & Information Security Law Blog, Hunton & Williams, 16 August [available at

https://www.huntonprivacyblog.com/2011/08/16/english-translation-of-perus-law-for-personal-data-protection-released/] accessed 30 November 2015.

Hunton & Williams (2015), "Germany Adopts a Draft Telecom Data Retention Law that Includes a Localization Requirement", Privacy & Information Security Law Blog, Hunton & Williams, 4 June [available at https://www.huntonprivacyblog.com/2015/06/04/germany-adopts-telecom-data-retention-law-includes-localization-requirement/] accessed 30 November 2015.

Jouanjean, M.A., (2019), "Digital Opportunities for Trade in Agriculture and Food," OECD Food, Agriculture and Fisheries Papers N° 124, OECD Publishing, Paris.

Kaplan, J.M. and K. Rowshankish (2015), Addressing the Impact of Data Location Regulation in Financial Services, Global Commission on Internet Governance (GCIG), *Paper Series*: No. 14, May.

Kuner, C. (2011), Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future, *OECD Digital Economy Papers*, No. 187, OECD Publishing, Paris, http://dx.doi.org/10.1787/5kg0s2fk315f-en .

López González, J. and J. Ferencz (2018), "Digital Trade and Market Openness", *OECD Trade Policy Papers*, No. 217, OECD Publishing, Paris, https://doi.org/10.1787/1bd89c9a-en.

López-González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", *OECD Trade Policy Papers*, No. 205, OECD Publishing, Paris, http://dx.doi.org/10.1787/524c8c83- en.

Mandel, M. (2017), "The Economic Impact of data: Why data is not like oil", Progressive Policy Institute, Accessed at https://www.progressivepolicy.org/publications/economic-impact-data-data-not-like-oil

Mandel, M. (2014), "Data, Trade and Growth", Progressive Policy Institute. Accessed at https://www.progressivepolicy.org/wp-content/uploads/2014/04/2014.04-Mandel_Data-Trade-and-Growth.pdf

Meltzer, J. (2015), "A New Digital Trade Agenda", E15 INITIATIVE, World Economic Forum and ICTSD, August.

Meltzer, J. (2014), "Supporting the Internet as a Platform for International Trade", Global Economy and Development, Brookings Institution, *Working Paper* 69, February.

McKinsey Global Institute (MGI) (2016), "Digital Globalization: The new era of global flows", McKinsey & Company, March 2016 available at: http://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/digital-globalization-the-new-era-of-global-flows on 22 March 2016.

National Board of Trade (2014), N*o Transfer, No Trade – the Importance of Cross-Border Data Transfers for Companies Based in Sweden*, Kommerskollegium, Stockholm.

National Board of Trade (2015), "No Transfer, No Production – a Report on Cross-Border Data Transfers, Global Value Chains, and the Production of Goods", Kommerskollegium, Stockholm.

Norton Rose Fulbright (2014), "Global data privacy: Directory", Norton Rose Fulbright, available at: http://www.nortonrosefulbright.com/files/global-data-privacy-directory-52687.pdf [accessed on 2 November 2015].

OECD (2017a), *Services Trade Policies and the Global Economy*, OECD Publishing, Paris, http://dx.doi.org/10.1787/9789264275232-en.

OECD (2017b), "Vectors of digital transformation", OECD internal document, Paris.

OECD (2013), *The OECD Privacy Framework 2013*, OECD Publishing, Paris, http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf.

OECD (2005), *OECD Guiding Principles for Regulatory Quality and Performance*, OECD Publications, Paris, https://www.oecd.org/fr/reformereg/34976533.pdf.

Posner, R.A. (1981), "The Economics of Privacy", *The American Economic Review*, Vol.71 (2), 405-409.

Reimsbach-Kounatze, C. (2015), "The Proliferation of "Big Data" and Implications for Official Statistics and Statistical Agencies: A Preliminary Analysis," *OECD Digital Economy Papers* 245, OECD Publishing, Paris, https://doi.org/10.1787/5js7t9wqzvg8-en.

Rowley (2007) "The Wisdom Hierarchy: Representations of the DIKW Hierarchy", *Journal of Information Science 2007*, Vol.33; 163. DOI: 10.1177/0165551506070706

Schwartz, P. (2009) "Managing global data privacy: Cross-Border Information Flows in a Networked Environment" Privacy Projects. www.provacyprojects.org

Schwartz, Paul M. and Solove, Daniel J., (2011) "The PII Problem: Privacy and a New Concept of Personally Identifiable Information" *New York University Law Review*, Vol. 86, p. 1814, 2011.

Schwartz, Paul M. and Solove, Daniel J., (2014) "Reconciling Personal Information in the United States and European Union", *California Law Review*, Vol 102 877.

Solove, D.J. (2006), "A taxonomy of privacy", *University of Pennsylvania Law Review*, Vol. 154 (3), 477.

Stone, S., J. Messent and D. Flaig (2015), "Emerging Policy Issues: Localisation Barriers to Trade", *OECD Trade Policy Papers*, No. 180, OECD Publishing, Paris, https://doi.org/10.1787/5js1m6v5qd5j-en

Telegeography (2015), "Global Bandwidth Research Service: Executive Summary", https://www.telegeography.com/page_attachments/products/website/research-services/global-bandwidth-research-service/0005/9474/gb15-exec-sum.pdf, accessed 11 April 2016.

The Economist (2017), "The world's most value resource is no longer oil, but data", 6 May.

USCIB (2015), "Forced Localization Matrix", United States Council for International Business, January.

USITC (2014), *Digital Trade in the US and Global Economies*, Part 2, USITC Publication 4485, August.

Annex A. International Data Protection Instruments

Convention 108

The *1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data*, commonly referred to as Convention 108 of the Council of Europe,[25] is a treaty protecting the right to privacy of individuals with respect to personal data which is automatically processed. To date, fifty-three states have committed to establish, under their own domestic law, sanctions and remedies for violations of the Convention's provisions. While individuals do not have a right of remedy directly under the Convention, claims between states with regard to how the Convention has been transposed could potentially be brought in front of the International Court of Justice.

A Protocol for the modernisation of the Convention was adopted by the Committee of Ministers on 18 May 2018 and opened for signature on 10 October 2018. When it will enter into force, it will repeal the 2001 Additional Protocol.

The 2001 Protocol established that states that are signatories to the Convention could not restrict the free flow of personal data between themselves, while with respect to third states, they had to restrict the flow of data and allow the transfer only where an adequate level of protection was ensured in the recipient entity, or where safeguards were in place.

The new Protocol of 2018 still provides that States that are party to the Convention should not restrict the flow of personal data among themselves, but introduces exceptions to this for cases where there is a risk that the transfer could lead to the circumvention of the provisions of the Convention, or where a party is bound by harmonised rules of protection shared by States belonging to a regional international organisation. This means that when the 2018 Protocol will enter into force, the signatories to the Convention will not be bound to ensure the free flow of data between themselves if one of the exceptions apply. The latter exception, for example, applies to the Member States of the European Union. However, as explicitly stated in the General Data Protection Regulation (EU) 2016/679, a third country's accession to Convention 108 and its implementation "will be an important factor when applying the European Union's international transfer regime, in particular when assessing whether the third country offers an adequate level of protection (which in turn allows the free flow of personal data)."[26]

[25] States party to the Convention are: Albania, Andorra, Armenia, Austria, Azerbaijan, Belgium, Bosnia and Herzegovina, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, European Union, Finland, France, Georgia, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Liechtenstein, Lithuania, Luxembourg, Malta, Monaco, Montenegro, Netherlands, Norway, Poland, Portugal, republic of Moldova, Romania, Russian Federation, San Marino, Serbia, Slovak Republic, Slovenia, Spain, Sweden, Switzerland, The Former Yugoslav Republic of Macedonia, Turkey, Ukraine, United Kingdom, Argentina, Burkina Faso, Cabo Verde, Mauritius, Mexico, Morocco, Senegal, Tunisia, Uruguay.

[26] Explanatory Report to the Protocol amending Convention 108, para 107.

Privacy Shield

The Privacy Shield Framework between the United States and the European Union is an adequacy decision which enables the flow of data from the European Union to the United States. Privacy Shield establishes a set of rules and principles that meet the EU adequacy requirements, and companies operating in the United States can voluntarily choose to be liable for such privacy protection under US law in order to be able to freely move personal data between the two economic areas, benefitting from the adequacy finding. Once they certify under the scheme, these protections become enforceable in the United States. The Privacy Shield also contains a number of commitments regarding the conditions under which the US authorities can access data transferred from the European Union.

APEC CBPR System

The APEC Cross-Border Privacy Rules (CBPR) System, in place since 2011, is a framework developed by APEC economies to promote the interoperability of privacy regulation through the enforcement of minimum standards. The CBPR System is not mandatory for APEC economies, and even when an economy adheres to it, companies can choose whether to seek certification under the System. To date, only six of the twenty-one APEC economies are participating to the System.

If an economy adheres to the CBPR System, it confirms its participation in the Cross-border Privacy Enforcement Arrangement (CPEA), a regional framework for enforcement cooperation in privacy matters. At the same time, it confirms its intention to use at least one Accountability Agent; that is, a third party oversight entity that must have been approved by the Joint Oversight Panel. In practice, adherence does not change the possibility for a member economy to retain its own privacy regulation, but it simply requires the appointment of a data protection authority (DPA) that is in charge of legally enforcing the privacy policies certified by the Accountability Agent.

Moreover, even if a company is located in an adhering economy, the company does not have to comply with the CBPR privacy framework unless the company itself voluntarily chooses to seek certification under the framework. In order to do this, the company must develop a privacy policy consistent with the framework to be reviewed by a competent Accountability Agent. Once the privacy policy is approved, the company is "white listed" as compliant with APEC's regional privacy standards. It therefore assumes liability for applying the relevant privacy practices to both the domestic relevant authority and an Accountability Agent.

The CBPR System only applies to data controllers, but a Privacy Recognition for Processors (PRP) has also been recently developed to help processors gain the trust of data controllers.