OECD publishing

Please cite this paper as:

Svantesson, D. (2020-12-22), "Data localisation trends and challenges: Considerations for the review of the Privacy Guidelines", *OECD Digital Economy Papers*, No. 301, OECD Publishing, Paris.
http://dx.doi.org/10.1787/7fbaed62-en

OECD Digital Economy Papers No. 301

Data localisation trends and challenges

CONSIDERATIONS FOR THE REVIEW OF THE PRIVACY GUIDELINES

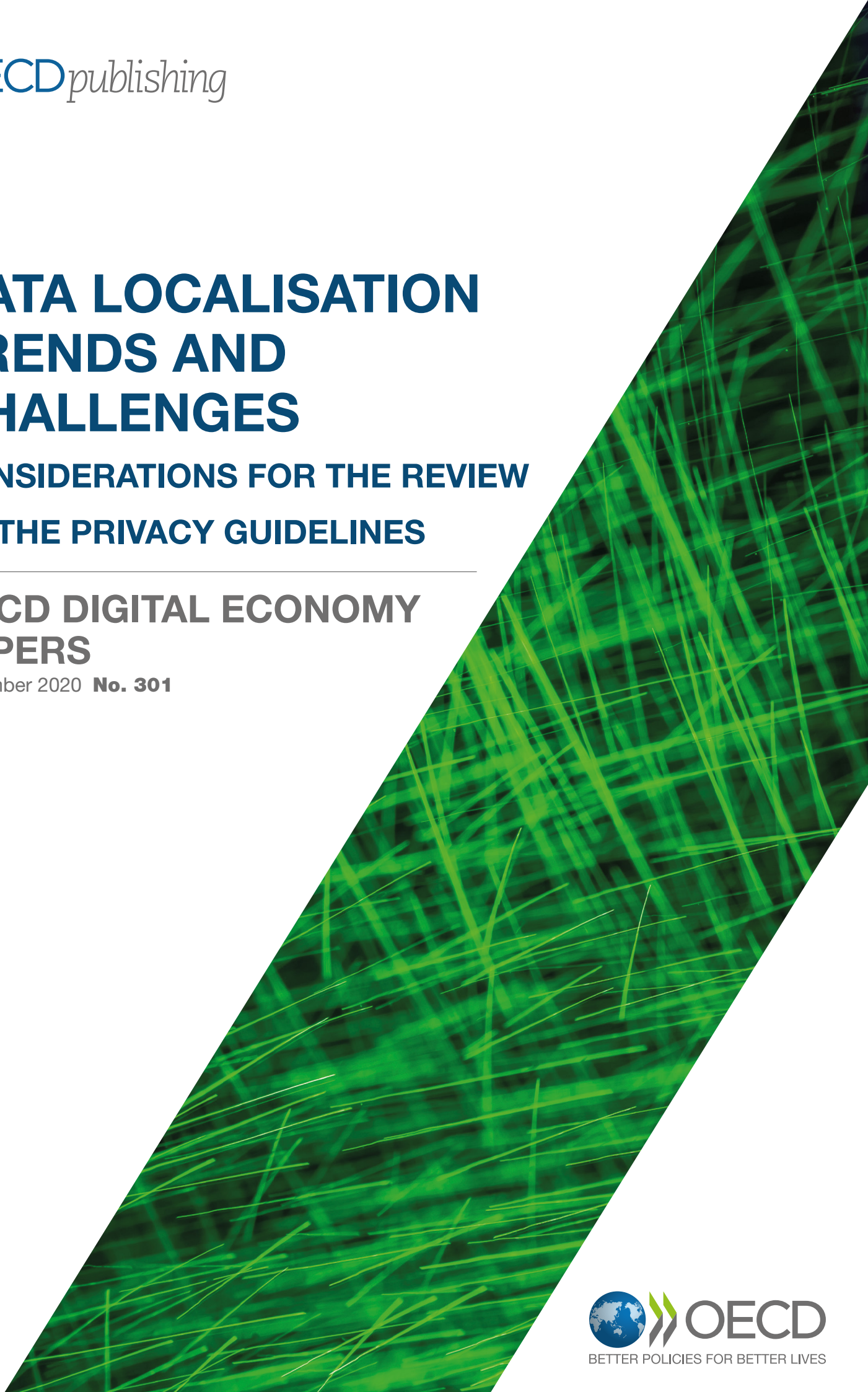
Dan Svantesson

OECD publishing

DATA LOCALISATION TRENDS AND CHALLENGES

CONSIDERATIONS FOR THE REVIEW OF THE PRIVACY GUIDELINES

OECD DIGITAL ECONOMY PAPERS
December 2020 **No. 301**



OECD
BETTER POLICIES FOR BETTER LIVES

Foreword

This report aims to review research on data localisation as an emerging impediment to data flows and data privacy protection. The report serves to inform the review of the implementation of the OECD Privacy Guidelines [OECD/LEGAL/0188] and guide further discussions amongst members of the OECD Working Party on Data Governance and Privacy in the Digital Economy (DGP), the OECD Secretariat and the Privacy Guidelines Expert Group that was formed to support the review.

This paper was drafted by Professor Dan Jerker B. Svantesson, Professor of Law, Bond University with feedback from Professor Christopher Kuner, Founder and Co-Director, Brussels Privacy Research Hub, Vrije, Universiteit Brussel , Elettra Ronchi and Lauren Bourke of the OECD Secretariat. It benefitted from the input of the expert group established to support the review of the OECD Privacy Guidelines and delegates of the Working Party on Data Governance and Privacy. The paper was further discussed at the virtual OECD Expert Roundtable on "Data localisation and Trusted Government Access to Data" held on 5-6 October 2020. The work was made possible by the generous contributions of Japan.

This paper should not be reported as representing the official views of the OECD or of its member countries. The opinions expressed and arguments employed are those of the author. It describes preliminary results or research in progress by the author and is published to stimulate discussion on a broad range of issues on which the OECD works. Comments on this paper are welcomed, and may be sent to the Directorate for Science, Technology and Innovation, OECD, 2 rue André-Pascal, 75775 Paris Cedex 16, France.

Note to Delegations:

This document is also available on O.N.E under the reference code:

DSTI/CDEP/DGP(2020)7/FINAL

Table of contents

Executive Summary

As defined in this Report, 'data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.

Such data localisation requirements have emerged as a major issue in transborder data flows and are of relevance for the OECD Privacy Guidelines, and the current review of the implementation of those Guidelines.

A review of trends within, and attitudes towards, data localisation amongst countries, consumers, industry and the expert community, highlights a complex situation in which data localisation is both seen as useful and as a significant threat and obstacle. Importantly, as some forms of data localisation are largely uncontroversial, while other forms are generally seen as problematic, a country's adoption of some form(s) of data localisation does not necessarily amount to an endorsement of other forms of data localisation.

Both the perceived benefits of, and the articulated concerns about, data localisation are diverse and go well beyond data privacy. Thus, the OECD Privacy Guidelines can only be expected to engage with certain aspects of the data localisation phenomenon. Yet, it is imperative that the approach to data localisation taken in the Guidelines is informed by, and mindful of, the broader context in which data localisation operates.

The Report argues that the OECD's current review of the implementation of the OECD Privacy Guidelines must address data localisation. To support such work, the Report makes nine recommendations (collated in the Annex).

The Report emphasises the need to recognise that data localisation has the potential to directly and significantly impact cross-border data flows (Recommendation 1), but suggests that, generally, the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation measures (Recommendation 2).

Further, the Report asserts that, whether a specific requirement is classed as a data localisation measure is not, on its own, determinative for whether such a requirement is incompatible with the OECD Privacy Guidelines (Recommendation 3). Rather, as data localisation may seek to protect data privacy in some cases, and undermine it in others, any assessment of the impact data localisation has on data privacy must be holistic and context-specific (Recommendation 4).

More specifically, the Report argues that, in the context of the OECD Privacy Guidelines, the proportionality test articulated in paragraph 18 should be considered a key mechanism for the evaluation of data localisation measures (Recommendation 5). In this context, the Report suggests that where a legal or administrative requirement is found to constitute a data localisation measure, and it amounts to a restriction to transborder flows of personal data under paragraph 18 of the OECD Privacy Guidelines, the assessment of whether it is proportionate (under that same paragraph) to the risks presented, ought to take into account multiple factors, and that the OECD should initiate work to map out what guidance, for the application of the proportionality test in paragraph 18 of the OECD Privacy Guidelines, that can be gained

from sources such as national laws, in international law and e.g. in EU law, WTO jurisprudence, academic literature and various trade agreements (Recommendation 6).

The Report also emphasises the relevance of the accountability principle of the OECD Privacy Guidelines paragraph 16 in the context of data localisation and recommends that the review of the OECD Privacy Guidelines engages with the potential compliance issues that data localisation may cause. (Recommendation 7).

Finally, the Report recommends that, either the Guidelines or the Explanatory Memorandum directly addresses data localisation (Recommendation 8) and provide a clear definition of data localisation; possibly as per the ad hoc definition introduced in this Report (Recommendation 9).

I. Introduction

The original explanatory memorandum to the OECD Privacy Guidelines (1980) observed that free flows of information between countries "have greatly increased in recent years and are bound to continue to grow as a result of the introduction of new computer and communication technology" (OECD, 2013, p. 39[1]). The correctness of the drafters' prediction is undisputable. Indeed, the degree of transborder data flows today may have been difficult to imagine in 1980. For example, recent figures suggest that: "The volume of data produced in the world is growing rapidly, from 33 zettabytes in 2018 to an expected 175 zettabytes in 2025" (European Commission, 2020, p. 2[2])[1]. We continue to be in the midst of an unprecedented information explosion in terms of the volume of data that are being collected, processed, shared, used and abused, much of which takes place via the Internet.

This growth in the processing of personal data[2] has been seen to go hand in hand with the globalisation of society; a phenomenon of which the Internet can be seen to be a cause and a component, as well as a reflection. It is repeatedly observed that globalisation presents unprecedented opportunities to boost economic growth (McKinsey Global Institute, 2014, p. 2[3]) (OECD, 2013[4]), and the opportunities for growth brought about by the combined forces of digitisation, digitalisation and globalisation hold particular promise to lift individuals in developing countries out of poverty (McKinsey Global Institute, 2014, p. 1[3]).[3]

At the same time, the past couple of years have been characterised by increasing international tension and an inwards focus amongst countries. The 2019 Internet & Jurisdiction Global Status Report observed that: "the international political climate has recently changed. There is a significant move away from international collaborative efforts and common goals, as more states adopt inward-looking policies and put their own immediate interests first" (Svantesson, 2019[5]). While numerous examples of international and regional collaboration continue, it seems possible that the noted trend of inward-looking policies will be both amplified and intensified by the current pandemic crisis that has gripped the world.

Yet, even in a climate of increasing emphasis on the domestic at the expense of the international, the necessity to transfer data across borders remains. It arises not just because of business needs, but for many other reasons as well. For example, individuals routinely expect that they will be able to communicate globally, which requires the ability to transfer data internationally. Governments and public authorities also exchange a vast amount of data on a global basis, much of which is done for routine purposes (e.g., exchanging information for social security and tax reasons, customs authorities exchanging data on shipments, health authorities keeping each other informed about the outbreak of diseases). Such data exchanges have become the lifeblood of the globalised society in which people live. For example, the current COVID-19 crisis demonstrates the need to transfer data across borders for purposes related to health research and other uses related to the public good (OECD, 2020[6]).

Data flows have brought risks, weaknesses and complications as well as benefits. For example, there has been an explosive growth in the scale and sophistication of cyber-attacks conducted via the Internet, and government access to and sharing of personal data may also create risks (Cate, Dempsey and Rubenstein, 2012[7]) (Cate and Dempsey, 2017[8]).[4] The 'Snowden revelations' – widely referred to as a key catalyst for data localisation (Chander and Le, 2015, p. 679[9]) (Fraser, 2016, p. 361[10]) (Selby, 2017, p. 216[11]) – have shown that common legal restrictions on data processing often do not apply, or are significantly different,

in the context of national security, intelligence services and law enforcement. Further, the hunger for ever-increasing data collection and the economic value of personal data have led to serious abuses by some private sector actors as well.

The regulation of data flows will continue to play a crucial role in how the Internet and society develop in the future. The Internet is now well-established as a truly international network of networks open to general usage, and the explosion of globalised electronic communications persists. In fact, in the context of the COVID-19 pandemic, we have seen increased reliance on online at the expense of the offline. This may well affect behaviour patterns long-term, meaning that we will continue to live an even greater segment of our lives online in the future as the world overcomes the pandemic. The pandemic has also exposed key weaknesses in data sharing and integration across public and private sources; clinical care and public health at local, state, national and international levels. For example, sharing patient-level data has been challenging because of an absence of interoperability and sharing of patient records, especially across geographical borders, and issues of individual consent and the need for ensuring anonymity. To this may be added the complications associated with ensuring an adequate level of data privacy in the context of contact-tracing apps (OECD, 2020[6]).

It also seems that we are on the verge of a further revolution brought about by the growth of data analytics, big data, AI, the processing of data in the 'cloud', and the widespread use of the Internet in connecting computers contained in everyday devices (the 'Internet of Things'). Many things are changing, but the crucial role of data remains a constant and this has resulted in a growing number of countries placing conditions on the transfer of data across borders or requiring that data be stored locally. As is discussed further below, some data localisation measures may fundamentally impact the transborder flow of data.

In the context of the review of the implementation of the OECD Privacy Guidelines, it is thus important to consider how the globalised data flows, and the governance thereof, is impacted by the trend of data localisation. To do so, this Report focuses on data localisation, and more specifically data localisation requirements (as opposed to voluntary data localisation). Part II provides an overview of the phenomenon of data localisation, its characteristics, uses and the concerns to which it may give rise. Part III outlines a set of nine recommendations (found in the Annex) on data localisation for the review of the implementation of the OECD Privacy Guidelines.

Thus, the Report aims to provide a detailed discussion of data localisation, facilitating the OECD engaging with this important issue in the context of the current review of the OECD Privacy Guidelines. This Report does not attempt to address holistically all aspects of data localisation. In particular, it does not attempt to thoroughly engage with the trade dimension of data localisation, including approaches taken in regional trade agreements and at the World Trade Organisation. Other, useful work has already been done in relation to trade and data localisation (Casalini and González, 2019[12]) (González and Jouanjean, 2017[13]). Rather, the Report focuses on data privacy and data governance considerations when it comes to data localisation, and suggests a roadmap for further work that can be conducted to ensure that transborder data flows, particularly amongst OECD Member Countries, are not impeded by data localisation.

II. Data localisation

A. What is data localisation?

The topic of data localisation is complex as it implicates multiple, and diverse, subjects ranging from Internet governance to international trade law, and from national security to regulatory reach and transparency. This means that a proper understanding of data localisation would need to involve many different committees within the OECD, including the Committee for Digital Economy Policy that is currently reviewing the OECD Privacy Guidelines. For example, the Guidelines are limited to personal data, but data localisation may relate both to personal data, and to non-personal data. This paper looks at these issues from the lens of the OECD Privacy Guidelines, notwithstanding the importance of data localisation in the context of other areas relevant to other OECD committees, such as trade-related issues or in the context of other areas that would not clearly and squarely fall within the OECD's mandate such as national security and law enforcement.

While data localisation may occur on a voluntary basis, this Report adopts the practice of using the term 'data localisation' as being synonymous with requirements for *mandatory* data localisation. There is not yet any universally accepted definition of what data localisation is, and while certain themes may be identified, data localisation may be categorised in a variety of manners (Kaplan and Kayvaun, 2015[14]; Casalini and González, 2019, pp. 24-26[12]). This definitional uncertainty is unhelpful and further work could usefully be directed at a systematic analysis of the various available definitions. However, drawing upon a range of definitions, and taking account of the context in which data localisation is discussed here, this Report advocates defining data localisation as follows:[5]

> *'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.*

Thus, data localisation as discussed here has several key characteristics. First, what we are dealing with are both **legal and administrative** requirements. Typically, data localisation is mandated by law, but it is also possible to speak of data localisation in the context of administrative requirements. For example, under the European Union's Regulation 2018/1807 on a framework for the free flow of non-personal data in the European Union, the term 'data localisation requirement' is specifically defined to include: "any obligation, prohibition, condition, limit or other requirement provided for in the laws, regulations or administrative provisions of a Member State or resulting from general and consistent administrative practices in a Member State and in bodies governed by public law, including in the field of public procurement".[6] Thus, under such a definition, it is the nature of the requirement that is of relevance rather than the pedigree of its creation; that is, a data localisation requirement is a data localisation requirement whether implemented by law or by a general and consistent administrative practice. This approach has several merits. Most importantly, it is the phenomenon of data localisation that needs to be examined not the manner in which such measures are implemented. A narrower focus – for example limited to data localisation mandated by law – could incentivise data localisation e.g. by administrative practices.

Relatedly, the fact that the definition is focused on requirements creates a need to be alert to the difference between **requirements**, on the one hand, and incentives, on the other. States may actively seek to attract data storage and processing by incentivising the transfer of such activities from outside their jurisdiction to inside their jurisdiction. For example, a February 2020 European Commission paper notes that: "The EU should take advantage of its effective data regulatory and policy framework to attract the storage and processing of data from other countries and regions" (European Commission, 2020, p. 24[2]). As long as such a strategy is pursued only by way of incentives, and not by legal or administrative requirements, it would not fall within the data localisation definition.

Furthermore, such legal or administrative requirement may mandate data localisation either **directly or indirectly**. This is important as the focus ought to be predominantly placed on the resulting regulatory environment rather than the means by which it is pursued. The important point is that such requirements must be **mandatory** within the system under which they are imposed. After all, businesses or industry may also voluntarily adopt data localisation practices, and such practices must be kept separate from the data localisation discussed here.

By simply referring to **data** the definition intends to emphasise that any type of data – whether personal or non-personal – may be subject to data localisation requirements. Having said that, data localisation laws are commonly specific about what type(s) of data, what sector and/or what types of actors, fall within the scope of those laws. For example, Australia's My Health Records Act 2012 (Cth), which requires data to be stored and processed exclusively within Australia, applies only to records held for the purposes of the My Health Record system.[7]

In the definition adopted above, focus is placed on data being required to be **stored or processed** on physical servers or digital storage units within a specified jurisdiction. In this context, it is important to distinguish this 'physical' element of data localisation from requirements that data be stored or processed within a given logical location, such as within a certain network.

The requirement that the data in question be stored or processed on physical servers or units **within a specified jurisdiction** makes clear that the phenomenon that the definition adopted above aims to address is the mandating of location. This is a distinct and separate matter from requirements relating to a prescribed level of protection, such as a data protection or cyber security standard that may be imposed as a condition for transborder data transfers. Thus, while a requirement that data may only be exported if a set standard is met may indirectly mean that certain entities *prefer* to limit the storage and processing to a certain jurisdiction, such a requirement is not necessarily a data localisation rule. Put simply, conditions being imposed on transborder data transfers is not the same as bans on transborder data transfers. While the two may be discussed together for some purposes, from a definitional perspective, it does not make sense to bundle them under the one label. Having said that, where requirements for conditional data export are set so high as to effectively amount to an absolute restriction on data exports akin to a mandatory legal or administrative requirement indirectly stipulating that data be stored or processed within a specified jurisdiction, that requirement may potentially fit within the definition of data localisation. This is discussed in detail below.

Further, the reference to within a specific jurisdiction departs from the practice of defining data localisation as requirements to store/process data within a specific country. The reference to within a specific jurisdiction is meant to highlight that data localisation may also be implemented, for example, on a regional basis.[8]

The definition advanced above extends the data localisation definition to situations where data must be **exclusively or non-exclusively** stored or processed within a specified jurisdiction. Yet, some other definitions of data localisation are even broader. For example, in a 2015 paper published by the Centre for International Governance Innovation and Chatham House, Kaplan and Rowshankish outline four main categories of data localisation requirements. From most to least stringent, Kaplan and Rowshankish's categories are:

> *"[1] Geographical restrictions on data export, which require data to be stored and processed within the country (i.e., "data copy cannot leave"). [2] Geographical restrictions on data location, which allow data to be copied outside of the country for processing, but require a replica in the local infrastructure (i.e., "data copy must stay"). [3] Permission-based regulations, which require institutions to gain consent from individuals for data transmission. [4] Standards-based regulations, which allow institutions to move data freely outside of the jurisdiction, but require them to take steps to ensure the security and privacy of customer data.*" (Kaplan and Kayvaun, 2015, pp. 1-2[14])

While such a broad all-encompassing definition has some advantages it also risks blurring issues that may be better discussed separately. For example, a requirement demanding data to be exclusively stored or processed within a specified jurisdiction gives rise to very different consideration to a requirement that personal data only be exported where certain security conditions are satisfied. In the light of that, while this Report discusses both matters in the context of distinguishing the two, the definition of data localisation advanced above is limited to, what in Kaplan and Rowshankish's terminology amount to 'data copy cannot leave' or 'data copy must stay' type data localisation rules.

Even with the definition advanced above, it is important for some purposes to keep in mind the distinction between exclusive ('data copy cannot leave') and non-exclusive ('data copy must stay') types of data localisation requirements. For example, for some types of data of national significance (such as historical records), it may be commonplace to require that a copy must always remain within the country. For physical records this has traditionally been accommodated in special archives and library collections, and countries may wish to mandate that such data – in digital form – be stored on designated domestic structures even though they may also be stored elsewhere. Thus, in this context, the policy considerations involved for a non-exclusive data localisation requirement may be different to those at play in the context of an exclusive data localisation requirement.

In contrast, while different policy considerations may be at play depending on whether we are dealing with exclusive or non-exclusive data localisation, both those types of data localisation may impose costs on operators, and both of them may affect cross-border data flows and impose costs on trade. For example, whether we are dealing with an exclusive, or non-exclusive, data localisation requirement, both necessitate the maintenance of technical infrastructure (and possibly staff) in the jurisdiction in question.[9]

This brings further attention to the importance of not bundling substantially different phenomena under one label. Thus, for some discussions, the definition of data localisation provided above is sufficient, but for other discussions, we need to clearly distinguish between, on the one hand, **exclusive ('data copy cannot leave') data localisation requirements, and non-exclusive ('data copy must stay') data localisation requirements.**

Finally, it must be emphasised that, the definition advanced above is merely put forward as a tool for delineating the relatively distinct phenomenon of data localisation. It neither distinguishing good from bad, nor legitimate from illegitimate. In other words, whether or not a specific legal or administrative requirement is 'good' or 'bad' is not determined by whether it fits within this definition. As this Report makes clear, some countries might consider that some data localisation measures are justified while others are not. Thus, assessments of the appropriateness of data localisation measures should not be carried out by reference to the proposed definition, but by having recourse to other concepts such as proportionality as recalled in the OECD Privacy Guidelines.

B. Trends in, and attitudes towards, data localisation

i. Amongst countries

Looking at State practice, there are clear indications that countries, and regions, see value in having data stored and processed locally. Indeed, the sheer number of data localisation laws are a testament to this attitude.

The lack of agreement on how to define data localisation means that there is limited value in seeking to ascertain the number of countries that have data localisation laws. Bearing this in mind, it can nevertheless be noted that an examination of key literature sees reference to some element of data localisation measures in, for example, the following 40 jurisdictions: Argentina, Australia, Belarus, Belgium, Brazil, Brunei Darussalam, Bulgaria, Canada, People's Republic of China (hereafter 'China'), Colombia, Denmark, the EU, Finland, France, Germany, Hungary, India, Indonesia, Iran, Jamaica, Kazakhstan, Korea, Luxembourg, Malaysia, the Netherlands, New Zealand, Nigeria, Peru, Poland, Russian Federation (hereafter 'Russia'), Sweden, Switzerland, Chinese Taipei, Thailand, Turkey, the United Kingdom, the United States, Uruguay, Venezuela, and Viet Nam.[10]

Importantly, it seems clear that not all these jurisdictions have data localisation requirements as defined above. Nevertheless, data localisation – broadly defined – is sufficiently widespread to necessitate it being considered in the context of the review of the implementation of the OECD Privacy Guidelines.

The OECD's current review of the implementation of the OECD Privacy Guidelines has involved a questionnaire on national and international developments (regulatory, policies, and technological) and on the relevance of the Privacy Guidelines. The questionnaire was circulated in April 2019 to all OECD Member countries and to non-Members who are Participants in the OECD Committee for Digital Economy Policy. The survey was completed by government officials, and thus does not (at least not directly) address challenges from a private sector perspective.

Twenty-nine countries responded to the questionnaire by the due date, set to 14 February 2020.[11] Of these, 11 countries (38% of respondents) responded to the questionnaire saying that they have provisions in their data governance and privacy regulatory framework concerning data localisation.

In some of these countries, only specific types of personal data were subject to a localisation requirement (for example, health records in Australia, national archives in Norway and data relevant to national security in Finland). Canada explained that for the public sector, its Direction for Electronic Data Residency requires that Protected B, Protected C and classified Government of Canada (GC) electronic data reside on approved servers in Canada or within the premises of a GC department abroad.[12]

While the figures above point to a relatively widespread adoption of measures, self-declared as data localisation, not all those measures fit within the definition of data localisation articulated above. As explained, requirements that data may only be exported under certain conditions – such as requirements relating to levels of data protection or cyber security standards – do not necessarily qualify as data localisation as defined here (although as noted, such requirements are covered in the Report in the context of distinguishing them from data localisation as defined here).

It is noteworthy that, in identifying the main challenges to transborder data flows, 10 countries responded that data localisation trends were one of the main challenges to data flows. That makes data localisation the 4th most highly rated challenge after 'uncertainty regarding legal privacy regimes' (19 countries), 'incompatibility of legal regimes' (16 countries) and 'time and resources required' (14 countries). Importantly, while specifically identified by 10 countries, data localisation may also be approached as an aspect of, and contributor to, the three most commonly cited challenges. In other words, data localisation contributes to uncertainty regarding legal privacy regimes, it creates a landscape of incompatibility of legal regimes and it adds to the time and resources required for legal compliance. From this perspective, the

challenges created by data localisation may, in fact, be more acutely felt than a superficial reading of the OECD questionnaire results suggests.

In the light of the discussion above, it seems possible to draw at least four conclusions of relevance for the OECD's current review of the implementation of the OECD Privacy Guidelines:

1. There is a need for a clear definition of what amounts to data localisation;
2. Some countries see benefits in, and have adopted, data localisation;
3. As some forms of data localisation are largely uncontroversial, while other forms are generally seen as problematic, a country's adoption of some form of data localisation cannot be seen as a necessary endorsement of other forms of data localisation; and
4. Countries see data location as one of the main challenges to transborder data flows.

ii. Amongst experts from industry, civil society, academia and international organisations

The industry attitude towards data localisation is exemplified in a recent publication by the Confederation of Danish Industry (DI). It notes that data localisation "make it difficult for companies to realise the potential of digitalisation" (Confederation of Danish Industry, 2018, p. 1[15]). The same publication:

1. Notes that "the world has seen a significant rise in digital protectionism the last decade"
2. Expresses concern "about the upward tendency in digital protectionism"
3. Highlights privacy as a fundamental right and key element in the confidence between companies and consumers. But notes that "the respect for privacy should not be misused as an excuse to impose measures that prevent legitimate movements of business-related data"; and
4. Stresses that, "Especially, SMEs are benefitting from the possibility of digital trade which saves resources and help them reach customers globally."

Importantly, this publication also provides real-world illustrations of how data localisation is impacting industry. One such illustration relates to the wind turbine industry (although data generated or used by wind turbines is generally not sensitive (i.e., not personal and arguably not a source of threat to national security either). The publication describes that:

> *"If a country decides to impose data localisation requirements, it becomes expensive for wind turbine manufacturers to provide services to the wind energy parks located in this country. The reason is that data localisation requirements will force wind turbine manufacturers to pay for a local data server. Depending on the extent of the data localisation requirements, wind turbine manufacturers will also have to process data locally. Such requirements provide local manufacturers with a significant competitive advantage since their data servers are already located in the country. Hence, data localisation requirements distort competition which leads to higher prices on wind energy.*
>
> *Secondly, free flows of data are important to improve productivity of wind systems. The fact that wind turbine manufacturers operate on global markets means that they in principle are able to conduct big data analyses in which they collect data from all of their machines in order to advance production of electricity. Such mechanisms are only possible to apply if wind turbine manufacturers are allowed to collect and store data from their foreign production on their main server. Thus, data localisation requirements are a serious obstacle to improve productivity."* (Confederation of Danish Industry, 2018, p. 2[15])

This is a particularly useful illustration as it relates to an industry not typically discussed in the data context. Other illustrations in the Confederation of Danish Industry's publication showcase the impact of data localisation for diverse industries including hearing aid manufacturers, manufacturers of analysis instruments for the food industry, supplier for minerals and cement industries, and multinational technology

company manufacturing hardware and software and providing IT-related consultancy services. At a minimum, the first of these examples involves transborder transfers of personal data.

More broadly, the 2019 Internet & Jurisdiction Global Status Report, published in November 2019 by the Internet & Jurisdiction Policy Network, gives insights into how the expert community,[13] including industry experts, views data localisation measures:

> *"When asked whether the increasing number of laws requiring data localization is part of the problem or part of the solution [in the context of cross-border legal challenges], 47% of surveyed experts indicated that this trend is part of the problem. 31% stated that it is both part of the problem, and part of the solution, while 9.5% took the view that this trend is neither part of the problem, nor part of the solution. Only 12.5% saw the trend as part of the solution."* (Svantesson, 2019, p. 165[5])

This brings attention to the strongly held concerns about data localisation requirements, but it also highlights that data localisation is seen as useful by some. The same Report notes that there are "clear sectoral and regional differences among surveyed experts' attitudes toward data localization laws" and more broadly, the Report concluded that: "the countries that are primarily receivers of internet services may – correctly or incorrectly – perceive data localization as a tool for power equalization" (Svantesson, 2019[5]).

iii. Amongst consumers

While the figures referred to above are focused on the attitudes of countries, industry and experts, there are also clear indications that individual consumers see a value in having data stored and processed locally. According to the 2019 version of the Global Survey on Internet Security and Trust – an international survey published annually – the majority (73%) of consumers wanted their online data and personal information to be physically stored on a secure server *in their own country* (CIGI-IPSOS, 2019[16]). At the same time, almost half (42%) of the respondents also indicated that they wanted their online data and personal information stored on physically secure servers *outside* their country.[14]

In the context of data localisation, it is also relevant to observe that, in the same survey, only 39% agreed with the statement: "It does not bother me that the data of firms in my economy sometimes goes outside of my economy" (CIGI-IPSOS, 2019, p. 11[16]). The figure for the same statement related to the data of the survey respondents' governments was 36%, suggesting that consumers care more about government data going outside their respective economies. Finally, 36% agreed with the statement that "It does not bother me that my data sometimes goes outside of my economy" (CIGI-IPSOS, 2019[16]).

C. Why are data localisation requirements imposed?

As can be expected, there is a range of reasons why countries may choose to impose data localisation requirements. Thus, to understand the phenomenon of data localisation, it is necessary to appreciate the diverse goals that are being pursued through data localisation requirements. Furthermore, as hinted at in the discussion above, there may be different reasons why a country adopts an exclusive ('data copy cannot leave') data localisation requirement, compared to why a country adopts a non-exclusive ('data copy must stay') data localisation requirement. Adding to the complications associated with mapping out the reasons data localisation requirements are introduced, countries may not always be entirely transparent as to their true motivations (Crowcroft et al., 2016, pp. 255-256[17]).

While the adage that 'data is the new oil' has largely fallen out of fashion, it does point to something of relevance for our context – at its most basic level, it reminds us that, similarly to control of oil, control of data provides both economical and geo-political advantages. Indeed, arguably the most basic reason for the increase in data localisation may be traced to the economic value of data. Data are more valuable today than ever before, and perhaps for psychological reasons, but also for practical reasons, countries

want to have what is valuable closer to them as it gives them a greater sense of control.[15] At the same time, it is of course true that just having a large stock of data stored locally is not valuable in and of itself.

i. Common motivations for data localisation

Common motivations for data localisation requirements may include data localisation:

1. in the pursuit of cybersecurity;
2. to limit foreign cyberespionage;
3. to assist law enforcement and national security agencies' access to data;
4. for the purpose of minimising and investigating cybercrime;
5. for the protection of personal data;
6. to cater for cyber-resilience;
7. to provide geo-political advantages;
8. in order to ensure government access to certain categories of data; and
9. to provide economical competition advantages.

Many of these motivations for the introduction of data localisation requirements are related, and indeed overlap. For example, stronger cybersecurity may arguably be pursued in order to minimise cybercrime, to limit cyber espionage, to enhance cyber-resilience, and to protect data privacy.

Physical access to the server on which data are stored may contribute towards enabling access to the data. This has caused concerns about having data stored overseas and has been used as the justification for exclusive data localisation requirements out of a concern for **cybersecurity**, to limit **cyberespionage**,[16] and for **the protection of personal data**.[17] Put simply, some exclusive data localisation requirements are implemented in order to hinder, or at least complicate, foreign access to the data of the country implementing data localisation.

However, in the light of the combination of encryption technologies,[18] and the possibility of remote access, just as physical access does not guarantee actual access to the data, lack of physical access does not exclude the possibility of access to the data. As correctly observed by Millard:

> *"From a technical perspective, physical access to a server or other device containing data is neither a necessary, nor a sufficient, condition for access to information in an intelligible form. On the other hand, logical access is both necessary, and may be sufficient, to provide access to data in an intelligible form, regardless of geographic location."* (Millard, 2015, p. 4[18])

This undermines the efficiency of data localisation as a tool for the purposes of limiting cyberespionage, and as a tool for the protection of personal data (in the limited context of excluding foreign access). It also undermines the efficiency of data localisation as a tool for cybersecurity in the sense of access-control. However, there are three functions/components typically attributed to cybersecurity. Cybersecurity aims to ensure confidentiality, ensure integrity, and ensure availability (the so-called CIA triad) (Villanova University, 2019[19]). The location of data remains an important, but not on its own determinative, consideration at least for cybersecurity's function of ensuring availability.

More broadly, it may be noted that, while critically important information systems rather than objects (e.g. data centres) are in focus when States define their cybersecurity agendas (Polcak and Svantesson, 2017[20]), the physical security of facilities hosting crucial data and/or systems is a component of cybersecurity and location is undeniably a consideration in the context of physical security. The relationship between data localisation, privacy enhancing technologies, and cybersecurity is a subject ripe for further

research. Any such research must be nuanced enough to recognise the three different functions/components of cybersecurity highlighted here.[19]

This discussion of cybersecurity overlaps with data localisation pursued for **cyber-resilience**. Where data is exclusively stored on a particular server, those who have physical access to that server may be able to make that data unavailable. Doing so may be a rather blunt tool given that disconnecting or destroying the server will also impact the availability of unrelated data. Nevertheless, for certain data types this cyber-resilience angle may be a motivator for either exclusive or non-exclusive data localisation requirements. More broadly, data localisation is being pursued with the express aim of ensuring resilience in the event of a country being, intentionally or unintentionally, cut off from the global Internet as in such an event access to data will to a great degree depend on their physical location. Additionally, given the **geo-political** significance of data, data localisation requirements may be pursued for the same reason that countries, for a long time, have sought to restrict the transfer of technologies that will pose a threat to national security or that will constitute an advantage to an enemy country.[20]

Data localisation is also implemented for the purpose of **minimising and investigating cybercrime** as locally stored data may be better protected against cybercrime, and as data being stored locally may, it is claimed (Selby, 2017, p. 230[11]), make it easier for **domestic law enforcement or national security agencies** to investigate crimes in relation to which the data is useful as evidence. However, many factors impact whether data is vulnerable to cybercriminals and location is merely one such factor, and not necessarily the most important factor. Further, the proposition regarding access to evidence arguably rests on an under-appreciation of the extensive use of encryption. In this context, it may be of interest to consider alternatives to data localisation as a means of legitimate law enforcement access to evidence. After all, there are already avenues for such access under Mutual Legal Assistance Treaties (MLATs) and progress is being made in facilitating direct law enforcement requests to the technology companies that often hold the data in question.[21]

Another aspect of data localisation as a tool to enhance law enforcement is found in its use to facilitate surveillance by domestic law enforcement or national security agencies. Frequently, this goal is less clearly, and less openly, articulated than the objectives discussed above. For example, in the context of Russia's September 2015 Data Localization Act, Federal Law No. 242-FZ it was emphasised that: "The main purpose of the law is to provide extra protection for Russian citizens both from misuse of their personal data by foreign companies and surveillance of foreign governments."[22] Yet there is widespread concern that the true motivations are found elsewhere. In particular, as is discussed in more detail below there are strong concerns that data localisation is being used as a tool for political repression, to silence dissidents and to facilitate their identification and oppression (Chander and Le, 2015, pp. 737-738[9]) (Byhovsky and Garrie, 2017, pp. 248-249[21]) (Fraser, 2016, p. 366[10]).

For China, for example, "[t]he Internet is regarded as one of the biggest threats to ideological security" (Liu, 2020, p. 96[22]) and an often-cited illustration of data localisation used for political repression is China's Cybersecurity Law, and specifically Article 37 that introduces a data localisation requirement (Livingston and Greenleaf, 2016, pp. 22-26[23]). Already prior to its introduction, this far-reaching data localisation requirement attracted widespread opposition (Yuxi, 2018[24]), and it has been observed that Article 37 threatens human rights while at the same time it is of highly questionable value for cybersecurity; i.e. the stated justification for introducing it in the first place (Access Now, 2017[25]). In fact, it has been suggested that this data localisation requirement may even undermine cybersecurity (Access Now, 2017[25]).

Data localisation is relatively widespread for the purpose of ensuring **access to certain categories of data** that are viewed as particularly sensitive or closely tied to an important governmental interest, such as passport records or financial records. Commentators have pointed to data localisation being pursued for such reasons for example in Germany, Denmark, Belgium, Finland, Sweden and the UK (Selby, 2017, p. 226[11]). Also, the GDPR permits, under strict conditions (subject to necessity and proportionality and notification to the Commission), Union or Member State law to limit data transfers based on important

reasons of public interest which has been interpreted to cover national databases of strategic importance, such as passport databases or electronic health records (Kuner, 2020, p. 855[26]). This type of data localisation requirement generally attracts far less concern and opposition than do most others.[23]

One of the common justifications presented for data localisation requirements is found in the **economic competition advantages** that may be gained: "Many governments believe that by forcing companies to localize data within national borders, they will increase investment at home. Thus, data localization measures are often motivated, whether explicitly or not, by desires to promote local economic development." (Chander and Le, 2015, p. 721[9])[24]

However, there seems to be a lack of empirical research as to whether or not data localisation does bring economic benefits, and assertions as to the economic advantages a country may gain from data localisation have not gone unchallenged. Indeed, as discussed below, the economic implications are an often-cited concern about data localisation. Commentators have pointed out that domestic weaknesses (e.g. in the power network) and conditions (e.g. high risks of earthquakes) may severely undermine the economic advantages of data localisation (Selby, 2017, p. 229[11]). Further, it has been argued that the indirect cost to the domestic economy broadly might outweigh the direct economic benefits gained by the local data storage/processing industry since:

> *"local data centres are likely to charge higher prices to local businesses and Internet users to store data as compared to the economies of scale enjoyed by the most efficient global data centre operators. Those higher costs would then create downstream comparative disadvantages for local Internet businesses, leading to an overall loss of efficiency in the local economy."* (Selby, 2017, p. 229[11])[25]

ii. Data localisation and the territoriality of jurisdiction in the online environment

The prevalent reluctance to explore alternatives to grounding jurisdiction in territoriality is a significant incentive for data localisation; that is, to the extent that jurisdiction over data is anchored in the location at which the data are located, data localisation may be motivated by a desire to **facilitate claims of jurisdiction.**[26] Somewhat similarly, where the location of data is used as a criteria for establishing jurisdiction over the holder of that data, the territoriality-focused thinking is an incentive for data localisation.[27] Thus, as noted by Chung "[t]he myth of localization as a precondition of legal jurisdiction is an aggravating element" (Chung, 2018, p. 208[27]).[28] However, as also noted by Chung, "[t]erritoriality has never been the sole ground for legal jurisdiction" (Chung, 2018, p. 208[27]), and indeed, territoriality has never been an appropriate ground for legal jurisdiction in the online environment.

In this context, Kuner questioned whether "since enforcement jurisdiction is primarily territorial, may the location of assets or equipment in the jurisdiction be justified as a way to make it easier to enforce local law?" (Kuner, 2014, p. 2094[28]).This is an important observation, but it may arguably be seen to conflate two distinct (yet related) issues; one being the issue of enforcement jurisdiction, the other being the issue of effective enforcement. The former relates to a country's rights. The latter is more of a practical consideration. At any rate, combining this with what was observed above, we can in fact identify three distinct situations where the emphasis on territoriality works as an incentive for data localisation:

1. Where the location of data is used as a criterion in assessing jurisdiction over the holder of those data;
2. Where the location of data is used to determine jurisdiction over those data; and
3. Where the location of data is utilised to enhance the effectiveness of enforcement actions.

In answering Kuner's question and starting with the question of enforcement jurisdiction, it is true that it has traditionally been anchored in territoriality (Ryngaert, 2015[29]). But the landscape is changing (Svantesson, 2019, p. 60[5]), and indeed has changed since Kuner's writing in 2015. Modern laws such as e.g. the US CLOUD Act,[29] do not attach great weight to the location of data as determining enforcement

jurisdiction. In fact, such a trend can also be seen in the data privacy context as is exemplified, for example, in the GDPR that makes clear that it "applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, *regardless of whether the processing takes place in the Union or not*."[30]

As to the efficiency argument, it is undoubtedly true that data localisation may aid the enforcement of local law e.g. due to the resulting presence of physical assets that may be seized. This has obvious practical advantages but also an economic dimension in that the cost of enforcement may be minimised. The latter aspect supports the notion that data localisation brings economic benefits, but at the same time it should be remembered that data localisation also imposes costs at several levels and the savings gained must be balanced with those costs.

The use of data localisation requirements as a means of enhancing the effectiveness of enforcement actions is part of a broader trend of localisation requirements. Another emerging, related, and potentially even more impactful, component of that trend is the phenomenon of 'rep localisation'. Rep localisation requirements mandate that foreign organisation maintain a physical representation in the country imposing the requirement (Svantesson, 2019, pp. 147, 148[5]). Thus, organisations cannot access foreign markets without first establishing a physical presence there. Examples of rep localisation requirements can, for example, be found in the GDPR[31] and in the Thai Personal Data Protection Act B.E. 2562 (2019).[32] Given the considerable scalability issues created by rep localisation, this is a matter with which the OECD may wish to engage in future work. Here it is sufficient to note the trend and its relation to data localisation.

To conclude the discussion of data localisation and the territoriality of jurisdiction in the online environment, the idea that a country has jurisdiction to regulate all that occurs in its territory for no other reason than that it -in some form – occurs in its territory simply does not fit with the society of today, characterised as it is, by constant, fluid, and substantial cross-border interaction and data flows, not least via the Internet. Indeed, there is a longstanding and clearly increasing recognition that strict territoriality is ill-equipped for today's modern society, online as well as offline. Furthermore, an examination of the sources most commonly relied upon to justify grounding jurisdiction in territoriality, reveals underlying core principles and practical considerations that are not anchored in territoriality.[33] Thus, taking a position against jurisdiction being fundamentally anchored in territoriality should perhaps be easier than it first may seem. Further, doing so does not mean the complete abandonment of territoriality. A territorial connection may still signal the legitimacy of a jurisdictional claim, just not on its own. Thus, given that the trend of data localisation is so strongly linked to the tradition of treating territoriality as the cornerstone of jurisdiction, the review could suitably, at least implicitly, take a position supporting a move away from grounding the concept of jurisdiction in territoriality.

iii. Data localisation as an aspect of data sovereignty

In the context of this Report, the topic of sovereignty is of significance for at least two reasons. First, in paragraph 4, the OECD Privacy Guidelines refer to 'national sovereignty' as a basis for exceptions to the Guidelines. Second, there is arguably a connection between the topic of data localisation and the increasing calls for 'data sovereignty' and related concepts.

Starting with the latter, there is a longstanding discussion of how the Internet impacts, and is impacted by, sovereignty. Attention to this topic seems to have intensified over the past couple of years, and this topic has sparked debates going to the very core of the meaning of sovereignty.[34] Calls for 'data sovereignty', 'information sovereignty', 'digital sovereignty', and ' technological sovereignty', are frequently made without much attention being directed neither at defining what these concept are meant to signify in practice, nor at the extent to which they are truly anchored in the international law concept of sovereignty, or mere rhetoric.[35]

Kuner has pointed to 'informational sovereignty' as a concept that arose already in the 1970s because of widespread unease with the breakdown of national regulatory borders caused by electronic data flows (Kuner, 2013, pp. 28-31[30]). Further, a July 2020 publication by the European Parliament Think Tank states that, in the EU context, 'digital sovereignty' refers to: "Europe's ability to act independently in the digital world and should be understood in terms of both protective mechanisms and offensive tools to foster digital innovation (including in cooperation with non-EU companies)" (Madiega, 2020, p. 1[31]).

Writing on the concept already in 1992, Österdahl observed that 'information sovereignty' is a former Soviet concept implying "that the State has a right to control the dissemination of information within its territory. The State according to this doctrine has the right to control the news flowing out of the country and the news coming in." Österdahl also noted that: "The existence of such a sovereignty is controversial, however. From a Western standpoint the doctrine of information sovereignty runs contrary to the existing human rights law of freedom of information because it allows general government interference in the news flow" (Österdahl, 1992, p. 137[32]).

Indeed, the relationship, or hierarchy, between sovereignty (including in the form of data, information, or technological sovereignty) and human rights is of crucial importance. The traditionally Western view that human rights override sovereignty, necessarily imposes limitations on what countries may do. However, for example, under former Soviet international law doctrine, sovereignty took priority over human rights (Österdahl, 1992, p. 136[32]). It is worthwhile recalling this background as more and more countries and regions call for data sovereignty, information sovereignty or technological sovereignty.

At any rate, as is highlighted, for example, in a Canadian discussion of data sovereignty, data localisation may be an ineffective measure to ensure data sovereignty:

> *In the public cloud environment, government data is entrusted to a third party that may be subject to the laws of a foreign country, even if the data resides in Canada. As such, the key risk to the GC [Government of Canada] with respect to data sovereignty is that foreign agencies can leverage laws in their home country to compel CSPs [cloud service providers] to turn over the GC's data* (Treasury Board of Canada Secretariat, 2018[33]).

To understand the calls for these types of sovereignty, it is useful to note the extent to which some countries feel disempowered due to technological inequalities and push back with claims of sovereignty. The *2019 Internet & Jurisdiction Global Status Report* points to five factors that, together, make a range of actors – developing countries, smaller countries and smaller internet actors – feel disempowered:

> *"1. There is a perception that, compared to developed countries, developing countries have less of a say in the approaches taken by the major internet actors;*
>
> *2. There is a perception that, compared to major internet actors, smaller internet actors have less of a say in the approaches taken by the regulators;*
>
> *3. There is a perception that both smaller internet actors and developing countries lack a voice in the international dialogue;*
>
> *4. Extraterritoriality allows dominant states to impose their laws on the world, while smaller states lack the standing and means to enforce their laws even domestically; and*
>
> *5. Legal approaches from developed countries are being replicated to such a degree that it impacts the sovereignty and self-determination of developing countries"* (Svantesson, 2019, p. 64[5]).

These perceptions may contribute to an environment in which countries implement data localisation measures in the pursuit of regaining control, often articulated as 'sovereignty', in relation to other countries and international bodies. Thus, an overarching concern, and an important component in alleviating the perceived need for data localisation, is that of ensuring that all relevant stakeholders feel that their voices have been heard in the international debates.

As hinted at by several of the motivations for data localisation discussed above, data localisation requirements may be seen by some as an aspect of the pursuit of data, information and/or technological sovereignty. Yet, it cannot be presumed that data localisation measures necessarily fall within the exceptions facilitated under the OECD Privacy Guidelines relating to national sovereignty (OECD, 2013[1]). Outlining the scope of the Guidelines, paragraph 4 states that:

> *"Exceptions to these Guidelines, including those relating to national sovereignty, national security and public policy ("ordre public"), should be:*
>
> *a) as few as possible, and*
>
> *b) made known to the public."*

Furthermore, even if data localisation may be an aspect of data, information and/or technological sovereignty, the application of this, or any similar, exceptions relating to national sovereignty would require evidence that what is being pursued under the rubric of 'data sovereignty', 'information sovereignty', 'digital sovereignty', and/or 'technological sovereignty' is truly anchored in the international law concept of sovereignty. Thus, countries must be restrictive in when they rely on sovereignty as a justification for limiting data flows catered for under the Guidelines.

Put differently, this discussion points to three matters that ought to be considered further in the context of paragraph 4:

1. Whether data localisation may be an aspect of data, information and/or technological sovereignty;
2. Whether what is being pursued under the rubric of 'data sovereignty', 'information sovereignty', 'digital sovereignty', and/or 'technological sovereignty' is truly anchored in the international law concept of sovereignty; and
3. Ultimately, whether data localisation measures may fall within the Privacy Guidelines' exceptions relating to national sovereignty.

These are doubtlessly complex questions. However, it would be ill-advised to think that they could simply be side-stepped or ignored. Given the fact that paragraph 4 specifically makes reference to sovereignty it cannot be excluded that a situation will arise in which such matters must be considered. Thus, this is a topic with which further engagement is needed. In fact, it may be appropriate for the OECD to initiate further studies of the impact of the new calls for digital sovereignty and the like more broadly than just in the context of data localisation.

D. Concerns about data localisation

The trend of data localisation has gained considerable attention and many critical and concerned voices have been raised against data localisation. Indeed, the OECD has long warned against the implications of data localisation measures that restrict data flows, emphasised that any restrictions should be proportionate to the risks, and taken a stance in favour of transborder data flows e.g.:

> *"Suppliers should have the ability to supply services over the Internet on a cross-border and technologically neutral basis in a manner that promotes interoperability of services and technologies, where appropriate. Users should have the ability to access and generate lawful content and run applications of their choice. To ensure cost effectiveness and other efficiencies, other barriers to the location, access and use of cross-border data facilities and functions should be minimised, providing that appropriate data protection and security measures are implemented in a manner consistent with the relevant OECD Guidelines and reflecting the necessary balance among all fundamental rights, freedoms and principles"* (OECD, 2011, p. 7[34]).

Driven by similar concerns, data localisation is restricted in several international or plurilateral instruments, such as the United States-Mexico-Canada Trade Agreement. Article 19.12 titled *Location of Computing*

Facilities mandates 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."[36] Having said that, it should be noted that such instruments typically also contain normal exceptions permitting data localisation in specific circumstances.[37] Another example are the "Horizontal provisions for cross-border data flows and for personal data protection (in EU trade and investment agreements)", adopted by the EU Commission in 2018, which provide that "cross-border data flows shall not be restricted between the Parties by… requiring the localisation of data in the Party's territory for storage or processing" (Article A(1)(ii)).

The Internet & Jurisdiction Policy Network's *2019 Global Status Report*, observes that: "several surveyed experts expressed the view that data localisation requirements represent a blunt, dated and inadequate approach to the [Internet jurisdiction] problem, and that it reflects a failure to resolve legal questions" (Svantesson, 2019, p. 165[5]).

Some commentators have gone as far as to suggest that data localisation requirements "run counter to the borderless reality of the internet" (Hodson, 2019, p. 579[35]). Indeed, such views are seemingly common. However, the term 'borderless' is both vague and loaded. Further, opponents of such notions may call for us to remember that this 'borderless reality' is: (a) a questionable description of the Internet of today, (b) arguably not a technical necessity for the Internet, and (c) thus not necessarily permanent. Thus, rather than expressing concerns by reference to the Internet's argued 'borderlessness', it may be more fruitful to examine in more detail what characteristics – commonly bundled under the borderlessness label – that are worth protecting. This may require further research.

At any rate, it is not surprising that the concerns expressed against data localisation are as multifaceted as are the motivations for data localisation. Furthermore, as hinted at in the discussion about the definition of data localisation, different concerns arise for different types of data localisation. Thus, also in this context must we distinguish between exclusive ('data copy cannot leave') data localisation requirements, on the one hand, and non-exclusive ('data copy must stay') data localisation requirements, on the other hand. Nevertheless, two general, relatively distinct categories of concerns are discernible, be as it may that some concerns cut across those categories.

i. Concerns about economic and social impacts

The economic and social impacts associated with data localisation – whether exclusive or non-exclusive – are some of the most frequently cited concerns. Indeed, several attempts have been made at estimating the cost of data localisation in different settings (Badran, 2018[36]) (Van der Marel, Lee-Makiyama and Bauer, 2014[37]) (Brehmer, 2018, pp. 932,933[38]). While no attempt is made here to estimate the direct or indirect costs of data localisation, it appears settled that data localisation does indeed impose a considerable cost on those forced to abide by data localisation requirements. That cost comes, for example, in the form of:

1. The cost of local employment and infrastructure investment;
2. The cost of efficiency losses such as disruptions to global consolidation plans and skill dilution, compared to using the best equipped and most skilled staff wherever they are located; and
3. The increases in compliance costs and the legal uncertainty that stems from the unpredictability of scope and application of data many localisation requirements.[38]

As commonly is the case, these costs are ultimately passed on to consumers. To this may be added the costs that may result from economic actors being discouraged from engaging in a given jurisdiction (Kaplan and Kayvaun, 2015, p. 1[14]). Such costs may include financial losses such as taxation losses, as well as societal costs, such as a population missing out on a valuable service.

Further, it has been suggested that, due to the high cost of compliance, data localisation may risk entrenching the position and power of the small number of already dominant companies that can afford,

and have the legal and technical expertise, to comply with multiple data localisation requirements (Svantesson, 2019, p. 166[5]). This may stifle innovation and limit competition.

Data localisation impacts the online environment, and indeed society more broadly, in a number of ways; many of which are a cause for concern. Commentators have great fears of the potential implications of widespread mandatory data localisation: "We should be aware that data localization tends to cause Galapagos syndrome, in which a short-term comfortable life in isolation leads to long-term extinction. This is particularly true in the market of electronic commerce, which is by its nature global" (Chung, 2018, p. 207[27]).

While, as noted above, data localisation is frequently justified by reference to the need to protect data privacy and to enhance the security of data, there is concern that data localisation caters for surveillance, and undermines both data privacy and the security of data. For example, there has been concerns expressed that data localisation will have a negative impact on data privacy "by creating greater government access to user data, minimizing the efficacy of corporate privacy and security controls, and expanding the corporate network" (Brehmer, 2018, p. 930[38]). This in turn points to data localisation as a potential tool for political repression: "strict data localisation laws can enable political oppression by bringing information under governmental control and threatening individual rights such as the rights to privacy, data protection, antidiscrimination and freedom of expression, and democratic values" (Fraser, 2016, p. 366[10]).[39] More broadly, it has been observed that: "data localisation requirements could actually increase privacy risks by requiring data to be stored in single centralised locations that are more vulnerable to intrusion" (Export Council of Australia, 2018, p. 33[39]). As to data security, the same report suggested that: "There are also numerous examples of data localisation creating issues for the resilience and security of data by making it susceptible to a single point of failure" (Export Council of Australia, 2018, p. 35[39]).

Furthermore, it has been argued that mandatory data localisation – whether exclusive or non-exclusive – may be seen as a form of data protectionism and an impediment to cross-border trade.[40] In this context, Chander and Lê suggest that: "protectionist policies barring access to foreign services only invite reciprocal protectionism from one's trading partners" (Chander and Le, 2015, p. 714[9]). Further, Brannon and Schwartz observes that data localisation "ultimately create smaller, less robust markets across the globe" (Brannon and Schwartz, 2018, p. 12[40]). Indeed, of the academic commentaries on data localisation, a great number of them focus wholly or predominantly on the trade law implications of data localisation (Chung, 2018[27]) (Hodson, 2019[35]) (Selby, 2017[11]). Some focus on specific industries, and Kaplan and Rowshankish, for example, assert that the implications of data localisation requirements "are particularly significant for banking" (Kaplan and Kayvaun, 2015, p. 1[14]) which suggests a need for further studies assessing data localisation in an industry-specific manner.

As already alluded to, data localisation has been viewed as a driver for fragmentation and balkanisation (Fraser, 2016[10]) of the Internet increasing the risk of the Internet being turned into a 'splinternet'. Indeed, in their seminal article on data localisation, Chander and Lê observe that: "Data localization would dramatically alter this fundamental architecture of the Internet" (Chander and Le, 2015, p. 681[9]). Further, a leading paper discussing Internet fragmentation notes that:

> *"Data localization in the form of domestic processing and residency requirements, and the blocking of certain data flows, introduces new forms of fragmentation on the Internet at the content and transactions levels. Moreover, depending on how it was done, localization in the form of changes to the Internet's routing arrangements could entail broader fragmentation"* (Drake, Cerf and Kleinwächter, 2016, p. 45[41]).

The exact meaning of 'fragmentation' is often unclear and subject to debate. Indeed, content and services are often targeted to Internet users based on their location. Thus, it could be said that this phenomenon already exists and is even embraced by many providers of goods and services.

The concerns about fragmentation are not new (Force Hill, 2012[42]), and some commentators resist the use of terms such as 'Internet balkanisation', finding it to be alarmist and believing that, to some extent,

this reflects a natural de-centralised expansion of the Internet (Maurer and Morgus, 2014[43]). Even those who are concerned about fragmentation admit that the technical and organisational complexity of the Internet means that it is not a concept susceptible to black or white definitions, and should instead be seen as a spectrum running from an Internet where the experience of every Internet user is the same regardless of geographic location, computer type, or any other distinguishing characteristic, to one where the experience is different for each user (Force Hill, 2012, pp. 11,12[42]). It, thus, seems that much work is needed to differentiate those aspects of fragmentation that are harmful from those that not only reflect, but indeed facilitate, the natural and growing diversity of the Internet.

Finally, the concerns about the impact of data localisation must also be seen in the light of an increasing reliance on Internet shutdowns. A leading project monitoring Internet shutdowns recorded at least 213 shutdowns in 2019 (Access Now, 2020[44]). Where data is exclusively stored in a particular country, and that country decides to shut down the Internet access within that country, access to that data is cut, worldwide, for the duration of the Internet shutdown.

ii. Concerns about feasibility

Even leaving aside the serious concerns about cost and impact that have been described above, there are also feasibility concerns associated with data localisation. Most obviously, any data localisation requirement presupposes that the data controller can determine the geographical location of the data under its control. However, this does not always correspond with the current technical practices when one considers data storage technologies such as so-called 'sharding': "Sharding is the process in which rows of a database table are held separately in servers across the world-making each partition a 'shard' that provides enough data for operation but not enough to re-identify an individual" (Chander and Le, 2015, p. 719[9]). Thus, sharding, while commonly seen as beneficial e.g. for data privacy protection, cannot be achieved with data localisation. This prompts the question of whether we should let data localisation prevent sharding, or whether current technical practices (such as sharding) should prevent data localisation.

More broadly, Kuan Hon and her co-authors have pointed out that:

> *"Multiple physical locations may be involved in the provision of just one cloud service from a single provider—locations of data centres used not just for persistent storage, but also for active processing operations, for backups or to improve service availability and performance, eg caches, content delivery networks/edge locations, or for storage of and operations on indexes of stored data and other metadata"* (Crowcroft et al., 2016, p. 264[17]).

Furthermore, data localisation – whether exclusive or non-exclusive – will doubtlessly be impacted by technological developments. For example, in most of the forms it takes, the uptake of blockchain runs contrary to data localisation due to the inherent de-centralised nature of such technologies. Further, it has been observed that:

> *"Today 80% of the processing and analysis of data takes place in data centres and centralised computing facilities, and 20% in smart connected objects, such as cars, home appliances or manufacturing robots, and in computing facilities close to the user ('edge computing'). By 2025 these proportions are likely to be inverted"* (European Commission, 2020, p. 2[2]).

With such a development, data localisation may become a less realistic option than it arguably is today, unless of course we accept that data localisation be a barrier for such technological developments.

In the light of this, while the limitations imposed by a technical impossibility has not always been the absolute barrier for law makers that one might have hoped, and while there is legitimacy in calls for technology being adjusted to comply with legal developments, great care should be taken before demanding what is not possible under current technologies.

Similar concerns may possibly arise in the context of the, at the time of writing, fast-developing contact tracing tools aimed at limiting the spread of the COVID-19 pandemic (OECD, 2020[6]). Data localisation measures requiring data to be exclusively stored in a particular country may potentially hinder cross-border interoperability, and it may be the case that any such data localisation requirements undermine systems designed to provide cross-border anonymity, or pseudonymity, given that some such systems rely on data being stored on the users' devices.

A related feasibility concern is the currently uncoordinated approach to data localisation on the international level. Countries are no doubt free to introduce conflicting data localisation requirements. However, placing data controllers in a situation where compliance with one country's law necessitates the violation of another country's law is counterproductive, and risks sparking unhelpful phenomena such as a 'race to the highest fines', and 'rep localisation' requirements (discussed above) as countries seek enforcement advantages (Svantesson, 2019, pp. 146-148[5]).

Finally as to the feasibility concerns, the Internet & Jurisdiction Policy Network's *2019 Global Status Report*, notes that survey respondents "raised concerns that forced data localization lacks scalability as an approach, and noted that data localization requirements do not change who is responsible for the data" (Svantesson, 2019, p. 165[5]). Put simply, if all countries introduce data localisation requirements, most organisations will find it too costly to comply with all countries' requirements. They will then prioritise based on which markets they see as most profitable and other such considerations. Poorer less developed countries would be at risk of missing out both on e.g. the goods and services offered by the respective organisations. If correct, this scalability issue may mean that data localisation practises end up widening the gap between those countries that are dominant in the online environment (typically richer more developed countries) and those that are struggling to reach their potential (typically poorer less developed countries).

III. Finding a way forward on data localisation

The discussion above has made clear that data localisation is a complex and multifaceted phenomenon. Both the perceived benefits of, and the articulated concerns about, data localisation are diverse and go well beyond data privacy. Thus, it is clear that the OECD Privacy Guidelines can only be expected to engage with certain aspects of the data localisation phenomenon. Yet, it is imperative that the approach to data localisation taken in the Guidelines is informed by, and mindful of, the broader context in which data localisation operates. This is important for ensuring consistency within OECD's work as data localisation is a relevant consideration for some other areas in which the OECD engages, such as international taxation. However, it is also important for the prospect of the type of cross-instrument harmonisation – and ideally interoperability (OECD, 2013[1]) – that should always be an underlying consideration in standard-setting international instruments such as the OECD Privacy Guidelines.

A. Recommendations on data localisation for the OECD Privacy Guidelines

Dating back already to the OECD's 1980 Guidelines, data privacy laws typically serve the dual purpose of: (1) ensuring the protection of personal data, and (2) facilitating privacy-respecting transborder data flows.[41] Since then, these have remained the consistent aims of the OECD Privacy Guidelines and several privacy instruments around the world. Data localisation – at least in the form of exclusive, or 'data copy cannot leave', requirements – may clearly amount to an obstacle for the pursuit of the latter of these goals and both exclusive and non-exclusive data location requirements potentially also impact aspects of the former e.g. in undermining the efficiency of technologies aimed at facilitating data privacy. Thus, the significance of data localisation for data privacy, and the fact that data localization has the potential to directly and significantly impact transborder data flows, are both beyond dispute.

Before it is possible to assess the relationship between data localisation and data privacy, it is first necessary to confront the central question of whether the requirements data privacy laws impose on transborder data flows amount to a form of data localisation. Thus, the first section below addresses that question. The second section below engages with the question of whether data localisation is 'good' or 'bad' for data privacy. The third section examines how the Guidelines' proportionality test provided applies to data localisation. The fourth section relates to the transborder application of accountability obligations. Finally, recommendations are made as to how the Guidelines and surrounding documents may be structures to address the data localisation issue.

Recommendation 1

It must be recognised that data localisation has the potential to directly and significantly impact cross-border data flows.

i. Are data privacy driven restrictions on transborder data flows data localisation?

Many jurisdictions have imposed conditions on transborder data flows under data privacy laws (Kuner, 2013[30]), and it seems that many commentators include those restrictions in the definition of data localisation. However, there is a significant difference between something being banned and something only being allowed under stated conditions. More specifically in our context, there is a significant difference between a requirement mandating that data be stored or processed in a specific jurisdiction, on the one hand, and conditions being imposed on the transfer of data to another country, on the other hand. Indeed, the need to differentiate between these matters has already been recognised in OECD works (Casalini and González, 2019, p. 24[12]). As noted above, bundling distinct phenomena under the one banner of data localisation introduces unnecessary complications. Ultimately, this hinders a fruitful nuanced discussion and adds to the risk of people speaking at cross-purposes. It is for these reasons, this Report recommends a narrower definition of data localisation, as outlined above.

As noted, under the definition advanced above, in general, the conditions that data privacy laws impose on transborder data transfers do not necessarily amount to data localisation. Yet, as also emphasised above, in extreme cases where the requirements for conditional data export are set so high as to effectively amount to an absolute restriction on data transfers those requirements may be seen to fit within the definition of data localisation.[42] Different people will come to different conclusions as to whether this leads to the result that the current conditions data privacy laws commonly impose on transborder data transfers nevertheless may amount to data localisation. Some commentators expressly assert that they do.[43]

To this may be added the issue of what Chander has termed ‘soft data localization’; a term he takes to refer to “a legal regime that puts pressure on companies to localize, not by directly requiring localization of data or processes, but by making alternatives legally risky and thus potentially unwise” (Chander, 2020, p. 2[45]). Thus, such ‘soft data localization’ could, for example, arise where the legal landscape is uncertain to the degree that data localisation is the only identifiable effective approach to comply with the law while other potential approaches to comply with the law may exist but have not yet been confirmed to be effective.

Against this background, and taking account of the discussion above of the components of the proposed definition of data localisation, it may be of value, for conceptual purposes, to distinguish between four different types of situations that may persuade an organisation to locate their data in a particular jurisdiction:

1. **Bans** – countries may ban the cross-border transfer of data.

2. **Conditions** – countries may impose conditions on the cross-border transfer of data.

3. **Uncertainty** (‘soft data localisation’) – countries may, intentionally or unintentionally, create an uncertain legal landscape in which data localisation is the only clearly safe mechanism for compliance.

4. **Incentives** – countries may provide incentives encouraging organisations to locate their data within those countries.

Of these, only the first type of situation – bans – clearly fits the proposed definition of data localisation. However, at least the second (conditions), and possibly also the third (uncertainty), type of situation may also fit the definition of data localisation in extreme cases. In contrast, it is difficult to imagine an instance of the fourth type of situation – incentives – meeting the thresholds so as to fit the proposed definition of data localisation.

Admittedly, ambiguities with respect to when a cross-border data transfer restriction would be regarded as an indirect data localisation requirement are not helpful. However, at least for the purpose of the OECD Privacy Guidelines, any anxiety sparked by the potential for a definitional 'grey zone' should be alleviated by recalling that the proposed definition of data localisation is merely aimed at creating conceptual clarity rather than to delineate what is allowed and what is not. The true test of whether a measure like data localisation conforms to the Guidelines ought to be deferred to the proportionality assessment under paragraph 18 of the Guidelines (discussed in detail below); that is, whether or not a specific requirement is classed as a data localisation measure or not is not determinative for whether or not such a requirement is incompatible with the OECD Privacy Guidelines.

Recommendation 2

In general, the conditions data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation.

Recommendation 3

Whether a specific requirement is classed as a data localisation measure is not, on its own, determinative for whether such a requirement is incompatible with the OECD Privacy Guidelines.

Nevertheless, given the extent to which data privacy is being used as a justification for data localisation measures by countries that traditionally have shown scant interest in data privacy, there may be reasons to, as clearly as is possible, distinguish such data localisation measures from genuine data privacy measures in the debates to be had. In other words, care must be taken not to lump together all data privacy driven data localisation measures into the one category. Further work may be useful in this context.

ii. Is data localisation 'good' or 'bad' for data privacy?

As illustrated above, the need for enhancing data privacy protection is presented as a distinct motivation for data localisation. But claims that data localisation is beneficial for data privacy have been met with two distinct objections that must be kept apart and addressed separately. The first is that data privacy predominantly is a cover for protectionism. The second objection is that data localisation undermines privacy.

In relation to the first of these objections – the suspicions of covert protectionism – Kuner has explained that:

> *"Differences in privacy protection and the understanding of fundamental rights between the European Union and the United States may cause some in the United States to regard European Union legal restrictions on data flows, and other European concerns about the data processing practices of U.S. companies, as protectionist; indeed, [former] President Obama seems to take this position. However, a review of the historical record concerning the evolution of data flow restrictions in E.U. data protection law indicates that they are based more on policy considerations, such as avoiding circumvention of the law and guarding against specific data processing risks in other countries, than on protectionism"* (Kuner, 2014, p. 2093[28]).

As highlighted by Kuner restrictions on transborder data flows may genuinely be motivated by data privacy concerns, and such data privacy concerns are not necessarily an insincere cover for protectionism.[44] The definition of data localisation advanced above will assist to a degree in this delineation. Yet, as already hinted at, whether a specific data privacy measure amounts to data localisation of a protectionist type objectionable under the OECD Privacy Guidelines may be most appropriately decided by reference to the proportionality requirement recognised in paragraph 18 of the Guidelines (discussed in detail below), a topic deserving further investigations.

As to the suggestion that data localisation undermines data privacy protection, this claim may in fact be reconcilable with the claim that data localisation is beneficial for data privacy. Data localisation can, as discussed above, arguably help protect a person's data privacy, to a degree, by limiting the prospect of data being accessed and misused by foreign law enforcement and national security agencies. This does not, however, preclude the possibility that the same person's data, for example, is being accessed – with assistance from data localisation requirements – by the government of the country in which the data is stored. In the light of the above, it is not fruitful to speak of data localisation as either exclusively 'good', or exclusively 'bad', for data privacy.

Given the fact that data localisation may support data privacy in some settings, and undermine it in others, any assessment of the impact data localisation has on data privacy must be context-specific. Thus, as noted by Kuner, the more productive path towards criticising data localisation is found in "articulating a normative argument in favour of a free Internet" (Kuner, 2014, p. 2098[28]). In other words, data localisation is most effectively countered by emphasising the benefits of facilitating privacy-respecting transborder data flows; i.e. the second function of data privacy laws.

Recommendation 4

As data localisation may seek to protect data privacy in some cases, and undermine it in others, any assessment of the impact data localisation has on data privacy must be holistic and context-specific.

iii. A proportionality assessment for data localisation

Paragraph 18 of the OECD Privacy Guidelines states that: "Any restrictions to transborder 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." At least in the context of personal data, the proportionality assessment called for in this paragraph is central in the assessment of whether a specific data localisation measure is compatible with the OECD Privacy Guidelines.

In more detail, this proportionality test has a direct, and unavoidable, relevance for exclusive – 'data copy cannot leave' – data localisation measures. Furthermore, it is arguable that it also impacts non-exclusive – 'data copy must stay' – data localisation measures; that is, where a party wishes to move data from one location to another but is forced to keep a copy at the original location, that may arguably amount to a restriction to the transborder flow of those data. Thus, in the context of whether a specific data localisation measure is incompatible with the OECD Privacy Guidelines, engaging with the proportionality assessment called for in this paragraph is not optional; at least not in relation to personal data.[45]

As is explained in the 2013 Supplementary Explanatory Memorandum, paragraph 18 implements a risk-based approach and the reference to restrictions being proportionate to the risks aims to ensure that any restrictions upon transborder data flows imposed by Member countries do "not exceed the requirements necessary for the protection of personal data" (OECD, 2013, p. 30[1]). Thus, as approached in the Supplementary Explanatory Memorandum, the proportionality test articulated in paragraph 18 is seemingly only applicable to requirements argued to be necessary for the protection of personal data. Where this

view is adopted, the proportionality test only applies to some forms of data localisation; namely those that are implemented specifically for the protection of personal data.

Looking at the text of paragraph 18 alone, however, no such limitation can be seen. It refers to *any* restrictions to transborder flows of personal data. Thus, judging by the text of paragraph 18 alone, it may apply more broadly to any situation in which data localisation is argued to amount to a restriction to transborder flows of personal data. This interpretation gives a broader mandate to paragraph 18.

The focus on proportionality is relatively common amongst legal instruments and guidance for how to apply a proportionality assessment in this context may be gained from various sources including the elements of proportionality that are used in national laws, in international law and e.g. in EU law, WTO jurisprudence, academic literature, and various trade agreements.[46] Thus, attention could be given to considerations such as (1) whether the measures to be enacted are likely to fulfil the objectives pursued, (2) whether there are any less restrictive measure that could be enacted, and (3) whether the measure in question stands in a reasonable relation to the intrusion it will cause.

Without pre-empting the question of whether these potential elements of proportionality are to be adopted for the purpose of the application of paragraph 18 of the OECD Privacy Guidelines, a few observation can be made so as to canvass potential considerations for future work.

As to the first – whether the measures to be enacted are likely to fulfil the objectives pursued –as illustrated in the discussion above, currently, it seems that more evidence is needed before it is possible to conclude that data localisation measures fulfil the objectives pursued in relation to several of its uses. Thus, it may be suspected that at least some data localisation requirements would not survive such a proportionality assessment, and thus may be incompatible with the Guidelines.

In assessing whether there are any less restrictive measure that could be enacted, as well as whether the measure in question stands in a reasonable relation to the intrusion it will cause, the proportionality assessment could usefully look beyond domestic considerations and also take account of the direct and indirect international implications of the measures. After all, in an interconnected world, where a specific domestic measure is adopted without regard for the international implications of that measure, unnecessary friction may be caused. The proportionality assessment has the potential to encourage countries to structure their data governance measures – including data localisation measures – in the manner that least impacts on other countries and on the international community.

Indeed, the proportionality assessment could usefully go as far as to take into account the 'scalability' of the measure in the sense of what might be the effect if other countries adopt the same approach.[47] Incorporating a scalability component in the proportionality assessment could bring several benefits. For example, in assessing whether the measure in question stands in a reasonable relation to the intrusion it will cause, different conclusions may be reached if only one country adopts that measure or if that measure is universally adopted. Indeed, incorporating scalability in the proportionality assessment may be seen as a matter of fairness and a step towards levelling the playing field between the more powerful and influential countries and developing countries.

Furthermore, in international law, much weight is given to State practice.[48] This ought to create a strong incentive for countries to pursue scalable universal approaches given that a broad uptake of their approaches legitimise those approaches. Nevertheless, if these international considerations are incorporated in the proportionality assessment, care should be taken to avoid the risk of unduly impairing countries' sovereignty to achieve legitimate policy objectives.

Much work lies ahead in examining what, if any, general principles, commonly applied in proportionality assessments, can usefully inform the application of paragraph 18 in the context discussed here. The OECD may wish to engage in this work as a matter of urgency since, prior to such work, it would be premature to exhaustively map out how the proportionality test of paragraph 18 impacts data localisation. Nevertheless, a few additional observations may be made as to the application of the proportionality test specifically in

the context of data localisation. For example, it may be useful for the proportionality test to be equipped to evaluate stated justifications for data localisation measures; that is, the proportionality test ought to be equipped to look behind the labels – such as data privacy or cyber security – countries attach to the justification for their data localisation requirements.

Evaluating the legitimacy of various justifications for data localisation is not an easy task, and as correctly noted by Kuner:

> *"This raises the issue of whether the definition of data nationalism [which Kuner discusses as synonymous with data localization] should be based on an objective or a subjective standard. For instance, is an initiative to protect privacy rights online to be classified as "protectionist" because it has the effect of restricting data flows, even if this was not its primary purpose? Or is there some element of intent required when classifying an initiative as protectionist?"* (Kuner, 2014, pp. 2089, 2097, 2098[28])

An objective standard focused on effects may be comparatively easier to work with and taking account of subjective intentions undoubtedly adds complications. Nevertheless, a proper assessment of the proportionality of data localisation should arguably incorporate, in Kuner's terms, both an 'objective' and a 'subjective' standard. This, it may be suggested, is best catered for by a *prima facie* objective standard focused on the effects of the requirement in question, creating a presumption that may be rebutted by reference to a second test focused on the relevant actor's intent (more of a subjective standard, although also intent may be assessed based on as objective criteria as is possible). Under such a structure, a country or region with, for example, a long-standing practice of protecting and upholding the data privacy of its citizens, both in a domestic and international context, may be able to point to this practice to rebut an effects-focused finding that its measures amount to a form of data localisation that otherwise would have fallen foul of the proportionality test in paragraph 18. In contrast, a country that lacks such a practise and instead has a record of domestic human rights violations may perhaps be unable to rebut such a finding.

A useful tool in making this distinction is arguably to look at whether the country in question has a defined right of data privacy that is upheld both in the context of international and domestic interferences. Where the data privacy interest is promoted as a justification for data localisation measures aimed at limiting foreign privacy violations, but not protected in relation to privacy-invasive domestic measures, it seems clear that it is the interests of the government in power rather than the citizens that primarily is being protected.

Recommendation 5

In the context of the OECD Privacy Guidelines, the proportionality test articulated in paragraph 18 should be considered a key mechanism for the evaluation of data localisation measures.

Recommendation 6

Where a legal or administrative requirement is found to constitute a data localisation measure, and it amounts to a restriction to transborder flows of personal data under paragraph 18 of the OECD Privacy Guidelines, the assessment of whether it is proportionate (under that same paragraph) to the risks presented, ought to take into account multiple factors, such as:

(a) the sensitivity of the data;

(b) the purpose and context of the processing;

(c) the extent to which it is demonstrated that the data localisation measure effectively achieves the goals for which it was introduced;

(d) whether there are any less restrictive measure that could be enacted;

(e) the direct and indirect, domestic and international, implications of the measures;

(f) evidence of intent where it is possible to establish; and

(g) the implications likely to arise if also other countries adopt the same measure ('scalability' as a consideration in the assessment of proportionality).

The OECD should initiate work to map out what guidance, for the application of the proportionality test in paragraph 18 of the OECD Privacy Guidelines, that can be gained from sources such as national laws, in international law and e.g. in EU law, WTO jurisprudence, academic literature and various trade agreements.

iv. Transborder application of accountability obligations

There is a clear trend of parties processing personal data remaining responsible and accountable for the processing even when they transfer data across national borders. This is affirmed in various national, regional and in international instruments like the OECD Privacy Guidelines (OECD, 2013, p. 16[1]).

It is important that obligations towards the data and the individuals to whom they pertain not be limited by national boundaries. As specifically declared in the OECD Privacy Guidelines paragraph 16: "data controller remains accountable for personal data under its control without regard to the location of the data" (OECD, 2013, p. 16[1]). This has potentially significant implications in the context of data localisation. First, it highlights that data localisation measures should not affect the accountability of data controllers. Second, the fact that data controllers remain accountable for personal data under their control without regard to the location of the data may constitute an incentive for data controllers to avoid contact with countries that impose data localisation combined with invasive data access regimes. After all, such contact may place the data controller in a position where compliance with one country's law (e.g. an invasive data access regime) necessitates the violation of another country's law (e.g. data privacy requirements).The OECD may wish to explore this potential for compliance difficulties in future work.

Recommendation 7

Data localisation laws, especially where they are combined with invasive data access regimes, may cause compliance issues for organisations since OECD Privacy Guidelines paragraph 16 mandates that "data controller remains accountable for personal data under its control without regard to the location of the data". The OECD could usefully examine this issue further in the review of the OECD Privacy Guidelines.

v. Guidelines or Explanatory Memorandum?

The above has emphasised that the OECD's current review of the implementation of the OECD Privacy Guidelines ought to take account of, and indeed directly address, data localisation as an issue. Maximum prominence will be given to the issue of data localisation if directly and expressly addressed in the Guidelines and explored in more detail in the Explanatory Memorandum. Alternatively, data localisation could be addressed in the Explanatory Memorandum.

Whether the Guidelines or the Explanatory Memorandum addresses data localisation the section addressing it ought to explore the topic in detail, and could usefully incorporate the definition of data localisation articulated above; that is:

> *'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.*

Recommendation 8

Either the Guidelines or the Explanatory Memorandum ought to directly address data localisation.

Recommendation 9

Either the Guidelines or the Explanatory Memorandum ought to include a definition of data localisation, possibly as follows:

'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.

VI. Conclusions

This Report has examined the phenomenon of data localisation. It has provided a definition of this phenomenon, highlighted trends in its use, discussed its motivations and examined the concerns with which it is associated. Particular attention has been placed on the relationship between data localisation and data privacy, and the Report has sought to hint at the role data localisation plays in the bigger context of data flow governance.[49]

The Report has demonstrated that data localisation is an important issue impacting transborder data flows and that the OECD's current review of the implementation of the OECD Privacy Guidelines ought to address data localisation. To that end, the Report makes nine recommendations, collated in the Annex below.

Annex

Box 1. Table of Recommendations

Recommendation 1

It must be recognised that data localisation has the potential to directly and significantly impact cross-border data flows.

Recommendation 2

In general, the requirements data privacy laws traditionally impose on transborder data transfers do not necessarily amount to data localisation.

Recommendation 3

Whether a specific requirement is classed as a data localisation measure is not, on its own, determinative for whether such a requirement is incompatible with the OECD Privacy Guidelines.

Recommendation 4

As data localisation may seek to protect data privacy in some cases, and undermine it in others, any assessment of the impact data localisation has on data privacy must be holistic and context-specific.

Recommendation 5

In the context of the OECD Privacy Guidelines, the proportionality test articulated in paragraph 18 should be considered a key mechanism for the evaluation of data localisation measures.

Recommendation 6

Where a legal or administrative requirement is found to constitute a data localisation measure, and it amounts to a restriction to transborder flows of personal data under paragraph 18 of the OECD Privacy Guidelines, the assessment of whether it is proportionate (under that same paragraph) to the risks presented, ought to take into account multiple factors, such as:

(a) the sensitivity of the data;

(b) the purpose and context of the processing;

(c) the extent to which it is demonstrated that the data localisation measure effectively achieves the goals for which it was introduced;

(d) whether there are any less restrictive measure that could be enacted;

(e) the direct and indirect, domestic and international, implications of the measures;

(f) evidence of intent where it is possible to establish; and

(g) the implications likely to arise if also other countries adopt the same measure ('scalability' as a consideration in the assessment of proportionality).

The OECD should initiate work to map out what guidance, for the application of the proportionality test in paragraph 18 of the OECD Privacy Guidelines, that can be gained from sources such as national laws, in international law and e.g. in EU law, WTO jurisprudence, academic literature and various trade agreements.

Recommendation 7

Data localisation laws, especially where they are combined with invasive data access regimes, may cause compliance issues for organisations since OECD Privacy Guidelines paragraph 16 mandates that "data controller remains accountable for personal data under its control without regard to the location of the data". The OECD could usefully examine this issue further in the review of the OECD Privacy Guidelines.

Recommendation 8

Either the Guidelines or the Explanatory Memorandum ought to directly address data localisation.

Recommendation 9

Either the Guidelines or the Explanatory Memorandum ought to include a definition of data localisation, possibly as follows:

'Data localisation' refers to a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.

References

Access Now (2020), *The #KeepItOn report on internet shutdowns in 2019*, https://www.accessnow.org/keepiton/. [44]

Access Now (2017), *A closer look at China's Cybersecurity Law — cybersecurity, or something else?*, https://www.accessnow.org/closer-look-chinas-cybersecurity-law-cybersecurity-something-else/. [25]

Australia (n.d.), *Competition and Consumer Act 2010 (Cth)*, https://www.legislation.gov.au/Details/C2020C00352. [58]

Australia (n.d.), *My Health Records Act 2012 (Cth)*, https://www.legislation.gov.au/Details/C2020C00372. [53]

Badran, M. (2018), "Economic impact of data localization in five selected African countries", *Digital Policy, Regulation and Governance*, Vol. 20/4, p. 337. [36]

Barak, A. (2012), *Proportionality: Constitutional Rights and their Limitation*, Cambridge University Press. [71]

Basu, A., E. Hickok and A. Singh Chawla (2019), *The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India*, https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf. [48]

Bhyovsky, I. and D. Garrie (2017), "Privacy and data protection in Russia", *rnal of Law & Cyber Warfare*, Vol. 5/2, p. 235. [50]

Brannon, I. and H. Schwartz (2018), "The New Perils of Data Localization Rules", *Regulation*, Vol. 41, p. 12. [40]

Brehmer, J. (2018), "Data Localization: The Unintended Consequences of Privacy Litigation", *American University Law Review*, Vol. 67/3, pp. 923-933. [38]

Bygrave, L. (2014), *Data Privacy Law: An International Perspective*, Oxford University Press. [69]

Byhovsky, I. and D. Garrie (2017), "Privacy and data protection in Russia", *Journal of Law & Cyber Warfare*, Vol. 5/2, p. 235. [46]

Byhovsky, I. and D. Garrie (2017), "Privacy and data protection in Russia", *Journal of Law & Cyber Warfare*, Vol. 5/2, p. 235. [21]

Capital Gold Exchange (Undated), *Why Are Countries Pulling Their Gold Out of America?*, https://capitalgoldexchange.com/why-are-countries-pulling-their-gold-out-of-america/. [52]

Casalini, F. and J. González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, Vol. 220, http://dx.doi.org/10.1787/b2023a47-en. [12]

Cate, F. and J. Dempsey (eds.) (2017), *Bulk Collection - Systematic Government Access to Private Sector Data*, Oxford University Press. [8]

Cate, F., J. Dempsey and I. Rubenstein (2012), "Systematic Government Access to Private Sector Data", *International Data Privacy Law*, Vol. 2/4, https://doi.org/10.1093/idpl/ips027. [7]

Chander, A. (2020), "Is Data Localization a Solution for Schrems II?", *Georgetown Law Faculty Publications and Other Works 2300*, p. 2, https://scholarship.law.georgetown.edu/facpub/2300. [45]

Chander, A. and U. Le (2015), "Data Nationalism", *Emory Law Journal*, Vol. 64/3, p. 677. [9]

Chung, C. (2018), "Data Localization: The Causes, Evolving International Regimes and Korean Practices", *Journal of World Trade*, Vol. 52/2, p. 187. [27]

CIGI-IPSOS (2019), *Global Survey on Internet Security and Trust 2019*, https://www.cigionline.org/sites/default/files/documents/2019%20CIGI-Ipsos%20Global%20Survey%20-%20Part%206%20Cross-border%20Data%20Flows.pdf. [16]

Confederation of Danish Industry (2018), *Danish cases on the importance of free flows of data across borders*. [15]

Crowcroft, J. et al. (2016), "Policy, Legal and Regulatory Implications of a European Only Cloud", *International Journal of Law and Information Technology*, Vol. 24, pp. 251-278. [17]

Drake, W., V. Cerf and W. Kleinwächter (2016), "Internet Fragmentation: An Overview", *World Economic Forum*, http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf. [41]

European Commission (2020), *A European Strategy for Data, Brussels, 19.2.2020 COM (2020) 66*, https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1593073685620&uri=CELEX%3A52020DC0066. [2]

European Union (n.d.), *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*, https://eur-lex.europa.eu/eli/reg/2016/679/oj. [60]

European Union (n.d.), *Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union*, https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R1807. [47]

Export Council of Australia (2018), *From Resource boom to Digital Boom: Capturing Australia's Digital Trade Opportunity at Home and Abroad*, https://www.export.org.au/publications/from-resource-boom-to-digital-boom-capturing-australias-digital-trade-opportunity-at-home-and-abroad. [39]

Force Hill, J. (2012), "Internet Fragmentation: Highlighting the Major Technical, Governance and Diplomatic Challenges for U.S. Policymakers", *Paper, Science, Technology, and Public Policy Program, Belfer Center*. [42]

Fraser, E. (2016), "Data Localisation and the Balkanisation of the Internet", *SCRIPTed*, Vol. 13, p. 359. [10]

Ginsburg, T. (2017), "Introduction to symposium on sovereignty, cyberspace, and Tallinn Manual 2.0", *American Journal of International Law Unbound*, p. 111. [66]

González, J. and M. Jouanjean (2017), "Digital Trade: Developing a Framework for Analysis", *OECD Trade Policy Papers*, Vol. 205, http://dx.doi.org/10.1787/524c8c83-en. [13]

Hodson, S. (2019), "Applying WTO and FTA Disciplines to Data Localization Measures", *World Trade Review*, Vol. 18/4, p. 579. [35]

Hodson, S. (2019), "Applying WTO and FTA Disciplines to Data Localization Measures", *World Trade Review,*, Vol. 18/4, p. 579. [49]

Information Technology Industry Council (n.d.), *ITI Data Localization Snapshot*, https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf. [55]

Kaplan, J. and R. Kayvaun (2015), "Addressing the Impact of Data Location Regulation in Financial Services", *Centre for International Governance Innovation and Chatham House (Paper Series)*, Vol. 14, pp. 1-2. [14]

Kuner, C. (ed.) (2020), *Articles 44-50*, Oxford University Press. [26]

Kuner, C. (2014), "Data Nationalism and Its Discontents", *Emory Law Journal*, Vol. 64, p. 2089. [28]

Kuner, C. (2013), *Transborder Data Flows and Data Privacy Law*, Oxford University Press. [30]

Kuner, C. et al. (eds.) (2020), *Article 27*, Oxford University Press. [62]

Kuner, C. et al. (eds.) (2020), *Article 3. Territorial Scope*, Oxford University Press. [61]

Liu, J. (2020), "China's data localization", *Chinese Journal of Communication*, Vol. 13/1, p. 84 at 96, https://doi.org/10.1080/17544750.2019.1649289. [22]

Livingston, S. and G. Greenleaf (2016), "Data Localisation in China and Other APEC Jurisdictions", *Privacy Laws & Business International Report*, Vol. 143, pp. 22-26. [23]

Lovelock, P. and J. Meltzer (2018), "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia", *Brookings Global Economy & Development Working Paper*, p. 113. [56]

Madiega, T. (2020), "Digital sovereignty for Europe", *European Parliamentary Research Service*, p. At 1. [31]

Maurer, T. and R. Morgus (2014), *Stop Calling Decentralization of the Internet 'Balkanization*, slate.com, http://www.slate.com/blogs/future_tense/2014/02/19/stop_calling_decentralization_of_the_internet_balkanization.html. [43]

McKinsey Global Institute (2014), *Global flows in a digital age: How trade, finance, people and data connect in the world economy*, https://www.mckinsey.com/~/media/McKinsey/Featured%20Insights/Globalization/Global%20flows%20in%20a%20digital%20age/Global_flows_in_a_digital_age_Full_report%20March_2015.pdf. [3]

Millard, C. (2015), *Forced Localization of Cloud Services: Is Privacy the Real Driver?*, https://ssrn.com/abstract=2605926. [18]

OECD (2020), *OECD Policy Responses to Coronavirus (Covid-19): Tracking and Tracing COVID: Protecting Privacy and data while using apps and biometrics*, https://www.oecd.org/coronavirus/policy-responses/tracking-and-tracing-covid-protecting-privacy-and-data-while-using-apps-and-biometrics/. [6]

OECD (2013), *Interconnected Economies Benefiting from Global Value Chains*, https://www.oecd.org/publications/interconnected-economies-9789264189560-en.htm. [4]

OECD (2013), *OECD Privacy Guidelines Supplementary Explanatory Memorandum*, http://oecd.org/sti/ieconomy/oecd_privacy_framework.pdf. [1]

OECD (2011), *OECD Council Recommendation on Principles for Internet Policy-Making*, http://www.oecd.org/sti/ieconomy/49258588.pdf. [34]

Office of the United States Trade Representative (2020), *Agreement between the United States of America, the United Mexican States, and Canada (7/1/20)*, https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between. [68]

Österdahl, I. (1992), *Freedom of Information in Question*, Iustus Förlag AB. [32]

Polcak, R. and D. Svantesson (2017), *Information Sovereignty – Data Privacy, Sovereign Powers and the Rule of Law*, Edward Elgar Publishing. [20]

Privacy, U. (n.d.), *Recommendation on the Protection and Use of Health-Related Data*, https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/FINALHRDDOCUMENT.pdf. [65]

Ryngaert, C. (2015), *Jurisdiction in International Law*, Oxford University Press. [29]

Savelyev, A. (2016), "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?", *Computer Law & Security Review*, Vol. 32, p. 138. [51]

Scharwatt, C. (2019), *The impact of data localisation requirements on the growth of mobile money-enabled remittances*, https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation. [70]

Schmitt, M. (ed.) (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2d ed.*, Cambridge University Press. [57]

Selby, J. (2017), "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", *International Journal of Law and Information Technology*, Vol. 25, p. 213. [11]

Svantesson, D. (2019), "Internet & Jurisdiction Global Status Report", *Internet & Jurisdiction Policy Network*, https://www.internetjurisdiction.net/uploads/pdfs/Internet-Jurisdiction-Global-Status-Report-2019-Key-Findings_web.pdf. [5]

Svantesson, D. (2015), "A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft", *American Journal of International Law Unbound*, Vol. 109, p. 69, https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft. [64]

Thailand (n.d.), *Personal Data Protection Act B.E. 2562 (2019)*. [63]

Treasury Board of Canada Secretariat (2018), *Government of Canada White Paper: Data Sovereignty and Public Cloud*, http://publications.gc.ca/collections/collection_2018/sct-tbs/BT22-213-2018-eng.pdf. [33]

United States (n.d.), *Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943)*.. [59]

United States (n.d.), *Trading with the Enemy Act of 1917 (TWEA) 50 U.S.C. S. 5(b) (1982 & Supp. IV 1986)*. [54]

Van der Marel, E., H. Lee-Makiyama and M. Bauer (2014), "The Costs of Data Localisation: A Friendly Fire on Economic Recovery", *European Centre for International Political Economy*, https://ecipe.org/publications/dataloc/. [37]

Villanova University (2019), *The History of Information Security*, https://www.villanovau.com/resources/iss/history-of-information-security/. [19]

Wright, J. (2018), *Cyber and international law in the 21st century*, https://www.gov.uk/government/speeches/cyber-andinternational-law-in-the-21st-century. [67]

Yuxi, W. (2018), *Chinese Data Localization Law: Comprehensive but Ambiguous*, The Henry M. Jackson School of International Studies, https://jsis.washington.edu/news/chinese-data-localization-law-comprehensive-ambiguous/ (accessed on 1 December 2020). [24]

Notes

[1] The paper relies on figures from a 2018 study by the International Data Corporation (IDC).

[2] "Personal data" is defined in the OECD Privacy Guidelines as "any information relating to an identified or identifiable individual (data subject)" (at para. 1(b)).

[3] Stating that "By 2025, 1.8 billion people around the world will enter the consuming class, nearly all from emerging markets, and emerging-market consumers will spend $30 trillion annually, up from $12 trillion today".

[4] For example, when governmental law enforcement entities access personal data held by the private sector.

[5] This definition is offered purely as an operational definition for the purposes of this paper and for generating further discussion. A full review of existing definitions of data localisation (for example, in trade agreements) is outside the scope of this paper. It may be useful for future work to identify, compare and analyse such definitions.

[6] Regulation (EU) 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union, at Art 3(5).

[7] My Health Records Act 2012 (Cth), at s. 77.

[8] See e.g. the discussions of a 'Europe-only cloud' (Kuan, H. et al., (2016) "Policy, Legal and Regulatory Implications of a European Only Cloud" 24 *International Journal of Law and Information Technology* 251). See also the more recent discussion of 'common European data spaces': "The EU should create an attractive policy environment so that, by 2030, the EU's share of the data economy – data stored, processed and put to valuable use in Europe - at least corresponds to its economic weight, not by fiat but by choice. The aim is to create a single European data space – a genuine single market for data, open to data from across the world – where personal as well as non-personal data, including sensitive business data, are secure and businesses also have easy access to an almost infinite amount of high-quality industrial data, boosting growth and creating value, while minimising the human carbon and environmental footprint. It should be a space where EU law can be enforced effectively, and where all data-driven products and services comply with the relevant norms of the EU's single market. To this end, the EU should combine fit-for-purpose legislation and governance to ensure availability of data, with investments in standards, tools and infrastructures as well as competences for handling data. This favourable context, promoting incentives and choice, will lead to more data being stored and processed in the EU." (European Commission, *A European strategy for data*, Brussels, 19.2.2020 COM(2020) 66 final, at 3-4).

[9] A full examination of the (potentially significant) trade costs of data localisation is outside the scope of this paper. For further analysis on this matter, see, e.g., 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>; 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>.

[10] Basu A. et al., (2019) "The Localisation Gambit: Unpacking Policy Measures for Sovereign Control of Data in India", The Centre for Internet and Society, India <https://cis-india.org/internet-governance/resources/the-localisation-gambit.pdf; Chander, A. & Le, U., (2015) "Data Nationalism", 64(3) *Emory Law Journal* 677; Chung, C-M., (2018) "Data Localization: The Causes, Evolving International Regimes and Korean Practices", 52(2) *Journal of World Trade* 187; Fraser, E. (2016) "Data Localisation and the Balkanisation of the Internet" 13 *SCRIPTed* 359; Selby, J., (2017) "Data localization laws: trade barriers or legitimate responses to cybersecurity risks, or both?", 25 *International Journal of Law and Information Technology* 213; Hodson, S., (2019) "Applying WTO and FTA Disciplines to Data Localization Measures", 18(4) *World Trade Review*, 579; Global Data Localization Laws: Overview by *Practical Law Data Privacy Advisor* (Thomson Reuters RESOURCE ID W-002-9187); Garrie, D. & Byhovsky, I., (2017) "Privacy and data protection in Russia", 5(2) *Journal of Law & Cyber Warfare*, 235; Savelyev, A., (2016) "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?", 32 *Computer Law & Security Review* 138; Kuan, H. et al., (2016) "Policy, Legal and Regulatory Implications of a European Only Cloud" 24 *International Journal of Law and Information Technology* 251; Kuner, C., (2014) "Data Nationalism and Its Discontents" 64 *Emory Law Journal* 2089; Brehmer, J., (2018) "Data Localization: The Unintended Consequences of Privacy Litigation." 67(3) *American University Law Review* 927; Hodson, S., (2019) "Applying WTO and FTA Disciplines to Data Localization Measures", 18(4) *World Trade Review*, 579; Kaplan, J. & Kayvaun, R., (2015) "Addressing the Impact of Data Location Regulation in Financial Services" Centre for International Governance Innovation and Chatham House, PAPER SERIES: NO. 14 — MAY 2015; Brannon, I. & Schwartz, H., (2018) "The New Perils of Data Localization Rules" 41 *Regulation* 12; Drake, W., Cerf, V. & Kleinwächter, W., (2016) "Internet Fragmentation: An Overview", World Economic Forum,, <http://www3.weforum.org/docs/WEF_FII_Internet_Fragmentation_An_Overview_2016.pdf>.

[11] 26 OECD Members (Australia, Canada, Chile, Colombia*, Denmark, Estonia, Finland, France, Iceland, Israel, Italy, Japan, Korea, Latvia, Lithuania, Luxembourg, Mexico, New Zealand, Norway, Portugal, the Slovak Republic, Slovenia, Switzerland, Turkey, the United Kingdom and the United States) and three non-Members (Brazil, Singapore and Thailand) (*Note that while Colombia is an OECD Member since 28 April 2020, it was not at the time of completing the questionnaire).

[12] While 'classified electronic data' is data that if compromised would reasonably be expected to cause an injury to the national interest, 'Protected B' and 'Protected C' electronic data is data that, if compromised, could cause serious or extremely grave injury to an individual, organization or government. See further: Treasury Board of Canada Secretariat, (2017), Direction for Electronic Data Residency, <https://www.canada.ca/en/government/system/digital-government/digital-government-innovations/cloud-services/direction-electronic-data-residency.html>. The Treasury Board Secretariat also notably made a statement that it has determined that "a commercial public cloud can, under certain conditions, offer sufficient protections for data up to and including the Protected B level": see Treasury Board of Canada Secretariat, "Government of Canada White Paper: Data Sovereignty and Public Cloud" (2018) <http://publications.gc.ca/collections/collection_2018/sct-tbs/BT22-213-2018-eng.pdf>.

[13] The Report is based on a large-scale data contribution from 150 key stakeholders from the Internet & Jurisdiction Policy Network from: States, internet companies, technical operators, civil society, academia

and international organizations. A full list of the contributing experts is provided in the Report (Svantesson, D., (2019) *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network, at 9-13).

[14] See the CIGI-IPSOS (2019) Global Survey on Internet Security and Trust. However, these results are seemingly difficult to reconcile as an overlapping amount of respondents simultaneously want their data to be stored on a secure server in their respective countries and on a secure server outside respective their countries. Perhaps survey respondents focused more on the idea of their data being stored on a 'secure server', than on the location of the server in question. Alternatively, the survey result suggest that a proportion of respondents wish for their data to be stored on multiple secure servers in different countries.

[15] A similar homewards trend can be seen e.g. in the context of gold reserves (*Why Are Countries Pulling Their Gold Out of America?)* <https://capitalgoldexchange.com/why-are-countries-pulling-their-gold-out-of-america/>).

[16] As far as espionage is concerned, it should be noted that, national laws may provide different rules for government access – whether by law enforcement or national security agencies – to locally stored data as compared to data stored abroad. Indeed, different agencies may be tasked with accessing data based on whether they are stored domestically or in a different country. Thus, keeping data locally may place it outside the immediate lawful reach of certain foreign agencies that could have accessed the data had they been stored in the foreign country.

[17] The claim that some countries make of data localisation being pursued as a measure to limit the threat of foreign access to the personal data of its citizens is the central theme in the narrative of data localisation – as defined above – as a privacy-friendly measure. As is discussed in detail below, this must be kept separate to claims of data privacy being enhanced by strict standards imposed on the transborder transfer of personal data.

[18] It may be noted in passing that, data securely encrypted today may be vulnerable to future advances in decryption techniques. Thus, restricting access arguably remains a security concern also for encrypted data.

[19] It is, for example, far too simplistic to conclude that data localisation "undermines cybersecurity" as e.g. Chander recently did (Chander, A., (2020) "Is Data Localization a Solution for Schrems II?", *Georgetown Law Faculty Publications and Other Works* 2300, <https://scholarship.law.georgetown.edu/facpub/2300>, at 2).

[20] See e.g. the US Trading with the Enemy Act of 1917 (TWEA) 50 U.S.C. S. 5(b) (1982 & Supp. IV 1986). Notably, this Act is only applicable in relation to specific designated countries, and in wartime.

[21] See further: the amendments to the Budapest Convention, the EU's e-evidence reform, the US Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943), and more generally the work of Internet & Jurisdiction Policy Network's Data & Jurisdiction Contact Group <https://www.internetjurisdiction.net/work/data-jurisdiction>.

[22] See, Savelyev, A., (2016) "Russia's new personal data localization regulations: A step forward or a self-imposed sanction?", 32 *Computer Law & Security Review* 138 (Citing November 12, 2014 Interview with the head of Roskonmadzor, Alexander Zharov), <http://82.rkn.gov.ru/news/news70654.htm> (in Russian), as referred to in Garrie, D. & Byhovsky, I., (2017) "Privacy and data protection in Russia", 5(2) *Journal of Law & Cyber Warfare*, 235, at 241.

[23] Compare e.g. to the list of data localization laws listed here: *ITI Data Localization Snapshot* <https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures1-19-2017.pdf>.

[24] Relatedly, data localisation is implemented in the pursuit of levelling the regulatory playing field: "Another driver of cross-border data flows has been based on the need to apply existing regulation to new digital entrants. The concern is that over-the-top (OTT) service providers that use telecommunications infrastructure do not pay license fees and are not subject to similar regulations governing their operations or their content. Evidence suggests that, contrary to the fears of many communications ministers, the impact of OTT entry is a positive one in terms of infrastructure investment." (Meltzer, J. & Lovelock, P., (2018) "Regulating for a Digital Economy: Understanding the Importance of Cross-Border Data Flows in Asia", Brookings Global Economy & Development Working Paper 113 at viii. See further at 24-25).

[25] See further: Chander, A. & Le, U., (2015) "Data Nationalism", 64(3) *Emory Law Journal* 677, at 722.

[26] For example, the *Tallinn Manual 2.0* provides that jurisdiction can attach on the basis of the location of data: "territorial jurisdiction applies to persons, natural and legal, involved in cyber activities that are present within a State's territory and to cyber infrastructure and data that are located on that territory." (internal footnote omitted) (Schmitt, M. ed., (2017), *Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations 2d ed.*, (Cambridge University Press), at 55).

[27] While largely discredited as a sole connecting factor justifying claims of jurisdiction, the location of data is still a criterion of relevance in some jurisdictional assessments. For example, in assessing whether a foreign company "carries on business in Australia" under the Australian Consumer Law (*Competition and Consumer Act 2010* (Cth), s. 5(1)(g)), the Federal Court of Australia made reference to the company's content being held on servers in Australia amongst six different criteria. (*Australian Competition and Consumer Commission v Valve Corporation (No 3)* [2016] FCA 196, paras 198-205. Somewhat similarly, the location of the host server is a non-determinative connecting factor for determining the extraterritorial reach of Canada's *Personal Information Protection and Electronic Documents Act* (A.T. v. Globe24h.com [2017] 4 FCR 310, paras 53-54)).

[28] As an example of this, Kuan Hon and her co-authors state that "One priority motivating Brazil's desire to require local storage of data was 'so that it could be subject to Brazilian laws'" (Kuan, H. et al., (2016) "Policy, Legal and Regulatory Implications of a European Only Cloud" 24 *International Journal of Law and Information Technology* 251, at 273).

[29] Clarifying Lawful Overseas Use of Data Act (CLOUD Act) (H.R. 4943).

[30] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Article 3(1) (emphasis added). Consider also Article 3(2), and see further: Svantesson, D., (2020) "Article 3. Territorial Scope", in Kuner, C. et al. (eds), (2020) The EU General Data Protection Regulation (GDPR): A Commentary, (Oxford University Press) pp. 74-99.

[31] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC, Article 27. See further: Christopher Millard & Dimitra Kamarinou, Article 27, in Kuner, C. et al. (eds), *The EU General Data Protection Regulation (GDPR): A Commentary*, (Oxford University Press), at 589-598.

[32] At section 37(5).

[33] To move away from grounding jurisdiction in the concept of territoriality, it may be proposed that: "In the absence of an obligation under international law to exercise jurisdiction, a State may only exercise jurisdiction where: (1) there is a substantial connection between the matter and the State seeking to exercise jurisdiction; (2) the State seeking to exercise jurisdiction has a legitimate interest in the matter; and (3) the exercise of jurisdiction is reasonable given the balance between the State's legitimate interests and other interests." (Svantesson, D., (2015) A New Jurisprudential Framework for Jurisdiction: Beyond the Harvard Draft, 109 *American Journal of International Law Unbound* 69 https://www.asil.org/blogs/new-jurisprudential-framework-jurisdiction-beyond-harvard-draft). This framework has already started gaining a degree of traction. (See e.g.: UN Special Rapporteur on the Right to Privacy, *Recommendation on the Protection and Use of Health-Related Data*, <https://www.ohchr.org/Documents/Issues/Privacy/SR_Privacy/FINALHRDDOCUMENT.pdf>) If adopted as the jurisprudential core of jurisdiction – based on which existing claims of jurisdiction are evaluated and on which new more detailed jurisdictional rules are developed – it may serve to liberate our thinking from the bounds of a territoriality principle that no longer serves us well and that leads to data flow hinderance such as the phenomenon of data localization.

[34] Consider, for example, the ongoing debate as to whether sovereignty is itself a binding rule of international law, or rather a principle of international law that guides State interactions but does not dictate results under international law (see e.g.: Ginsburg, T., (2017) "Introduction to symposium on sovereignty, cyberspace, and Tallinn Manual 2.0" 111 *American Journal of International Law Unbound*, 205–206; and Wright, J., (2018) *Cyber and international law in the 21st century*. Retrieved from https://www.gov.uk/government/speeches/cyber-andinternational-law-in-the-21st-century).

[35] See e.g.: European Commission, A European strategy for data, Brussels, 19.2.2020 COM(2020) 66 final, at 16 noting that: "The Commission will use its convening power as well as EU funding programmes to strengthen Europe's technological sovereignty for the data-agile economy."

[36] United States-Mexico-Canada Agreement, Article 19.12.

[37] See e.g.: United States-Mexico-Canada Agreement, Article 32.1.

[38] In their 2015 paper, Kaplan and Rowshankish report that "executives reported that they have severe difficulties gaining a clear and comprehensive view of the full set of regulations. Many are worded so vaguely that it is impossible, they say, to predict what is and is not allowable. In some countries, regulators have given different answers to different institutions, making it difficult to find relevant precedents." (Kaplan, J. & Kayvaun, R., (2015) "Addressing the Impact of Data Location Regulation in Financial Services" Centre for International Governance Innovation and Chatham House, PAPER SERIES: NO. 14 — MAY 2015, at 2).

[39] Indeed, Kuner has called for assessments of data localisation to take account of the underlying values of democracy and legality, including by reference to international human rights instruments, such as the Universal Declaration of Human Rights of 1948 (UDHR) and the International Covenant on Civil and Political Rights of 1966 (ICCPR), that – as he points out – "protect the freedom to transfer data 'regardless of frontiers.'" (Kuner, C., (2014) "Data Nationalism and Its Discontents" 64 *Emory Law Journal* 2089, at 2096).

[40] As an example of this, Hodson points to how Indonesia in 2012 "introduced wide-reaching data localization measures as part of the Government's strategy to correct its trade deficit and improve infrastructure." (Hodson, S., (2019) "Applying WTO and FTA Disciplines to Data Localization Measures", 18(4) *World Trade Review*, 579, at 581).

[41] See e.g.: Bygrave, L., (2014) *Data Privacy Law: An International Perspective (*Oxford University Press), at 121 and Millard, C., (2015) "Forced Localization of Cloud Services: Is Privacy the Real Driver?" *IEEE Cloud Computing*, Available at SSRN: <https://ssrn.com/abstract=2605926>, at 2, noting: "a key stated objective of almost all international initiatives to promote harmonization of data privacy rules has been to facilitate the free movement of personal data between States that are prepared to make a commitment to enforce certain, more or less basic, data protection principles.".

[42] See also: Casalini, F. and J. González (2019), "Trade and Cross-Border Data Flows", *OECD Trade Policy Papers*, Vol. 220, http://dx.doi.org/10.1787/b2023a47-en, at 22 stating: "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."

[43] "Although it is seldom stated that the EU data protection rule has the purpose of data localization, it is not denied that the strict condition for cross-border transfer has the effect of encouraging data localization." Chung, C-M., (2018) "Data Localization: The Causes, Evolving International Regimes and Korean Practices", 52(2) *Journal of World Trade* 187, at 191.

[44] For an in-depth examination of the very detailed approach taken to cross-border data flows in the EU's GDPR, see: Kuner, C., "Articles 44-50", in Kuner, C. et al. (eds), (2020) *The EU General Data Protection Regulation (GDPR): A Commentary*, (Oxford University Press), at 755-862.

[45] While the discussion here is focused on the proportionality assessment featured in paragraph 18 of the OECD Privacy Guidelines, calls for proportionality in the context of data localization are common, see e.g.: Scharwatt, C., (2019) "The impact of data localisation requirements on the growth of mobile money-enabled remittances" GSM Association <https://www.gsma.com/mobilefordevelopment/wp-content/uploads/2019/03/GSMA_Understanding-the-impact-of-data-localisation.pdf>.

[46] See generally regarding the use of proportionality in different legal systems, Barak, (2012), *Proportionality: Constitutional Rights and their Limitation* (Cambridge University Press), and for example, Article 14.13 of the Comprehensive and Progressive Agreement for Trans-Pacific Partnership.

[47] Compare to the 'global south impact assessment' advocated in Svantesson, D., (2019), *Internet & Jurisdiction Global Status Report 2019*, Internet & Jurisdiction Policy Network, at 64: "it is arguably reasonable to expect lawmakers in those countries that commonly influence policy and law developments globally to conduct what may be termed a 'global south impact assessment', assessing: (1) what impact their approaches will have in the global south, and (2) what will happen if the global south adopts their approaches."

[48] See in particular: *Statute of the International Court of Justice*, Article 38(1)(b).

[49] Please also refer to the similar analysis of data localisation and privacy in terms of trade, which is conducted by OECD Trade Committee (i.e. Trade and Cross-Border Data Flows (2019)).