WPS8431

Policy Research Working Paper 8431

International Data Flows and Privacy

The Conflict and Its Resolution

Aaditya Mattoo
Joshua P. Meltzer

WORLD BANK GROUP
Development Economics
Development Research Group
May 2018

Policy Research Working Paper 8431

Abstract

The free flow of data across borders underpins today's globalized economy. But the flow of personal data outside the jurisdiction of national regulators also raises concerns about the protection of privacy. Addressing these legitimate concerns without undermining international integration is a challenge. This paper describes and assesses three types of responses to this challenge: unilateral development of national or regional regulation, such as the European Union's Data Protection Directive and forthcoming General Data Protection Regulation; international negotiation of trade disciplines, most recently in the Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP); and international cooperation involving regulators, most significantly in the EU-U.S. Privacy Shield Agreement. The paper argues that unilateral restrictions on data flows are costly and can hurt exports, especially of data-processing and other data-based services; international trade rules that limit only the importers' freedom to regulate cannot address the challenge posed by privacy; and regulatory cooperation that aims at harmonization and mutual recognition is not likely to succeed, given the desirable divergence in national privacy regulation. The way forward is to design trade rules (as the CPTPP seeks to do) that reflect the bargain central to successful international cooperation (as in the EU-US Privacy Shield): regulators in data destination countries would assume legal obligations to protect the privacy of foreign citizens in return for obligations on data source countries not to restrict the flow of data. Existing multilateral rules can help ensure that any such arrangements do not discriminate against and are open to participation by other countries.

This paper is a product of the Development Research Group, Development Economics. It is part of a larger effort by the World Bank to provide open access to its research and make a contribution to development policy discussions around the world. Policy Research Working Papers are also posted on the Web at http://www.worldbank.org/research. The authors may be contacted at amattoo@worldbank.org and JMeltzer@brookings.edu.

International Data Flows and Privacy:
The Conflict and Its Resolution

Aaditya Mattoo and Joshua P. Meltzer*

Keywords: data protection, privacy, globalization, trade, WTO
JEL codes: F13, F15, K24, L86

*World Bank and Brookings Institution, respectively. We have benefited from the comments of Cameron Kerry, Hamid Mamdouh, and Juan Marchetti and financial support from the World Bank's Multi-Donor Trust Fund for Trade and Development and Strategic Research Program, and from the Brookings Institution's David M. Rubenstein Special Initiative. The findings in this paper do not necessarily represent the views of the World Bank's Board of Executive Directors or the governments they represent. Any errors or omissions are the authors' responsibility.

International Data Flows and Privacy:
The Conflict and Its Resolution

Contents

I. INTRODUCTION 3
II. THE EU APPROACH TO PRIVACY 6
III. THE IMPACT OF EU PRIVACY REGULATION ON EXPORTERS: THE EXAMPLE OF INDIA 12
IV. THE TREATMENT OF PRIVACY UNDER CURRENT AND PROPOSED TRADE RULES 16
The WTO 16
Korea-US FTA 18
Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP) 19
The EU's Proposed Approach in its Trade Agreements with Other Countries 20
V. INTERNATIONAL REGULATORY COOPERATION ON PRIVACY AND DATA FLOWS 21
The OECD Privacy Guidelines 21
The Council of Europe Data Protection Convention and Additional Protocol 22
Asia Pacific Economic Cooperation (APEC) 22
The E.U.-U.S. Privacy Shield 24
VI. A PROPOSED APPROACH: BUILDING ON THE CPTPP AND THE PRIVACY SHIELD 24
VII. CONCLUSION 28
VII. Bibliography 30

I. INTRODUCTION

The ability to move data freely across borders underpins a growing range of economic activity and international trade. McKinsey estimated that cross border data flows were 45 times larger in 2014 than in 2015, and around 12 percent of international trade in goods is over global e-commerce platforms such as Alibaba and Amazon (Manyika et al., 2016). The US International Trade Commission estimates that in 2014, global digital trade, including of data-processing and other data-based services, led to a more than 3.4 percent increase in US GDP, by increasing productivity and lowering the costs of trade (ITC 2014). Overall, data flows are estimated to have increased world GDP by about 10 percent over the past decade (McKinsey 2016). These estimates are plausible because data flows have facilitated the diffusion of knowledge and technology, and enabled the fragmentation of production of goods and services across countries, resulting in gains from an ever finer international division of labor. Data flows are also the basis for potentially transformative developments, ranging from additive manufacturing, which could change trade in goods into trade in design, to cloud computing, which is already changing trade in IT products into trade in computer services. Furthermore, big data analytics, which rely on data gathered from across jurisdictions, are revolutionizing industries from banking and insurance to health and retail, and supporting the development of artificial intelligence.

However, international data flows are also raising concerns. The provision online of search, communication, health, education, retail and financial services relies on, or could lead to, the collection of personal data. The global nature of the internet means that such data can be quickly and easily transferred to third parties in other jurisdictions. This transfer can undermine domestic privacy goals when the personal data of citizens flows to jurisdictions which do not offer them comparable levels of privacy protection. This concern can prompt domestic regulators to limit the free flow of data across borders. For example, in October 2015, the Court of Justice of the European Union declared invalid an arrangement that facilitated data flows between Europe and the United States (which was subsequently renegotiated). The ruling came after privacy advocate Max Schrems brought a case against Facebook in Ireland, its European headquarters, saying his privacy had been violated by the US National Security Agency's mass-surveillance programs, first revealed by whistle-blower Edward Snowden.

Privacy protection is not a new issue. In the 19th century Samuel Warren and Louis Brandeis, concerned about the potential for media to intrude on personal lives wrote about a "right to be left alone" (Warren and Brandeis 1890). Protecting privacy became increasingly important post WWII, as governments' increasing use of personal data combined with new computing power to process the data. The developments led to various government reviews of privacy protection. In 1980, the OECD produced *Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data* – reflecting an OECD consensus on how member countries should handle and protect personal data.

More recently, in response to the dramatic growth of international data flows, the EU has implemented the world's most legally comprehensive data protection regime. The 1995 Data Privacy Directive (the Data Directive) will be replaced by the more ambitious General Data Protection Regulation (GPDR) on 28 May 2018. Since EU efforts to achieve its privacy goals can be circumvented when data are sent to other jurisdictions with lower levels of privacy protection, the EU Directive and Regulation make it illegal to

transfer personal data outside the EU unless privacy is adequately protected in the data destination country, including with respect to the rights of the data subject. In practice, this has meant a privacy regime equivalent to the EU, as has been confirmed by the Court of Justice of the European Union (Schrems v. Data Protection Commissioner 2015). In the absence of such protection, the EU allows data to be transferred internationally using model contracts that effectively bind the recipient of personal data to provide privacy protection equivalent to that if the data had remained in the EU. Personal data can also be transferred across borders within a single company that has accepted binding corporate rules on privacy. In all instances, the party transferring the data outside the EU is responsible for ensuring that the receiving party protects the personal data to the level required by EU law.

Just as data flows have produced economic benefits, restrictions on international data flows are likely to have economic costs. In the extreme case of a complete ban on exporting personal data from the EU to the United States, EU GDP has been estimated to decline by around 1 percent, EU exports to the United States by around 5 percent (because of higher costs of services inputs for EU manufacturing), and EU services imports from the United States by about 20 percent (Bauer et al 2013). In the less extreme and currently prevailing regime, each of the options for the transfer of personal data outside the EU – binding corporate rules and model contracts – too impose significant costs of compliance, especially in developing countries. The consequence, as we will discuss later, is reduced developing country exports of data-based services to the EU, which include data processing, information and computer services, valued at $7 billion in 2015, and other business services worth $43 billion. In cases where countries qualify for national adequacy or firms accept binding corporate rule options, exports to other jurisdictions may also decline because of the resulting increase in the national or firm-level costs of data processing.

Is unilateral action by the EU likely to spur similar privacy protection in other countries and lead to global regulatory convergence? Probably not, because the EU's conception of privacy as a fundamental human right reflects its own history and cultural trajectory, which many other countries do not share. For example, the EU regime is in part a reaction against the use by the Nazi's of records of personal data to carry out genocide and the Stasi's reliance on state records to establish a totalitarian state in East Germany. Even where other countries consider privacy a human right, it tends to be balanced against other values, such as free speech, in ways that lead to different levels of privacy protection than in the EU.[1] In the United States, greater emphasis is placed on the constitutional right to free speech and the right to privacy is accordingly more limited than in the EU (Bennett 2012, 169). In India too, while the High Court has recognized a constitutional right to privacy, it has also stated that this right needs to be balanced against the constitutional right to free speech (Justice KS Puttaswamy v. Union of India and Ors 2017*).*

Regulatory convergence is also unlikely because national privacy protection can have economic costs – quite apart from those arising from restrictions on international data flows – and the relative importance of these costs can differ across countries.[2] Asymmetries in information between two parties

[1] Even the EU Data Protection Directive Article 7(f) balances the right to privacy with other "legitimate interests pursued by the controller." As the ECJ has explained, this "necessitates a balancing of the opposing rights and interests concerned."

[2] Members of the Fortune 500 would need to spend on average $16 million each to avoid falling foul of the EU's General Data Protection Regulation according to estimates by the International Association of Privacy Professionals and EU, a professional services reform, reported in the Financial Times ("Global groups face big bills to comply with new privacy rules," 20 November 2017). Each company is expected to hire on average five dedicated privacy employees (e.g. data protection officers) and another five employees to deal partially with the new rules. Financial services and technology companies face the biggest compliance costs.

to a transaction distort the functioning of markets, e.g. in banking, insurance, or labor markets broadly, and privacy protection perpetuates such asymmetries. But fuller information can in some cases lead to less egalitarian outcomes – e.g. higher interests in loans for some borrowers, higher insurance premia for some people, and lower wages for some workers. In other cases, fuller information – e.g. in the form of consumer credit histories – may improve access to financial services for the less privileged. Limiting access to and use of personal data also dampens the scope for realizing economies of scale in the exploitation of big data, and hence limits the economic potential of the internet. Countries differ in how they strike a balance between efficiency and equity and in how much they value public services and economic activity that erode individual privacy. Therefore, even though privacy is a global concern, different national positions are emerging on optimal privacy protection.

The tension between international data flows and divergent national privacy standards has provoked two types of international responses: negotiation of trade rules and cooperation between regulators. The rules of the World Trade Organization (WTO) cover all measures, including a country's privacy law, that affect international trade and prohibit discrimination between trading partners and in favor of domestic services and service suppliers when a country has made the relevant commitments. However, the WTO's General Agreement on Trade in Services (GATS) provides an exception for measures necessary to secure compliance with laws that are otherwise consistent with the GATS relating to "the protection of the privacy of individuals in relation to the processing and dissemination of personal data" (GATS Article XIV(c)). The chapeau to Article XIV limits the exception to measures that do not lead to "unnecessary and unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services." While the WTO panels and appellate body have in other cases made judgements on whether a measure was necessary to achieve a specific objective, doing so in the context of the politically sensitive issue of privacy protection is probably asking too much from an already strained WTO dispute settlement system. Resolving trade and privacy issues using international trade rules that limit only the data source country's freedom to regulate and ask nothing of the data destination country is not politically sustainable.

In parallel, regulators are also cooperating to find ways of achieving desired levels of privacy protection without undermining the internet's economic and trade potential. For example, a 2013 update to the OECD Guidelines specifically recognized the impact of cross-border data flows on privacy as well as their economic and social benefits and called on OECD Members to "support the development of international arrangements that promote interoperability among privacy frameworks that give practical effect to these Guidelines" (OECD 2013).

However, traditional regulatory cooperation through harmonization and mutual recognition is not only unlikely but by itself insufficient to ensure international data flows. Harmonization and mutual recognition of national regulations do enable firms to realize economies of scale by averting the need to fragment operations to conform to differing regulations. But identical or mutually acceptable regulations do not by themselves address the central problem raised by international data flows. To protect the interests of their citizens, regulators in each country need to influence the behavior of data-handling entities located outside their jurisdictions; and the regulators in other jurisdictions who have control over these entities are not mandated to look out for the interests of citizens from other countries. Even if each country had the same national regulations, this gap between regulatory responsibility and regulatory authority would remain.

We argue that the way forward is to design trade rules, as in the recent Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), that reflect the bargain central to successful

international regulatory cooperation, as in the EU-US Privacy Shield. Data destination countries would promise to protect the privacy of foreign citizens in return for source countries committing not to restrict the flow of data. While this goal may not be immediately attainable for a large group of countries, we spell out a set of intermediate steps that are likely to be feasible for different sets of countries. We also discuss how the interests of countries that are left out of such arrangements can be protected by existing multilateral rules on recognition agreements.

This paper is structured as follows. Section II analyzes the EU privacy regime with a focus on its impact on cross-border data flows. Section III discusses the impact of the EU privacy regime on India, a major data processing destination, and what India would need to do to be deemed adequate under the EU Directive and GDPR. In this part, we also discuss the costs of compliance with the EU regime and the impact on services exports. Section IV examines how privacy is dealt with under the rules of four representative international trade agreements, the WTO, the Korea-US FTA, the recent CPTPP, and the EU's proposed approach to trade agreements with other countries. Section V provides an overview of attempts to promote regulatory convergence and cooperation on privacy. Here we discuss the OECD, APEC and European Data Protection Convention approaches. We also analyze the Privacy Shield Agreement, which provides an alternative mechanism to allow cross-border data flows. In Section VI, we propose an approach that builds on the CPTPP and the Privacy Shield and could eventually form the basis of a multilateral initiative. Section VII concludes.

II. THE EU APPROACH TO PRIVACY

The EU Data Protection Directive adopted in 1995 governs personal data protection in the EU. As a 'Directive', implementation is left to EU member states, and in practice, member states vary widely in their enforcement of the Data Directive. The European Commission will replace the Data Directive with the GDPR in May 2018 (EU 2018). Under EU law, a Regulation is directly applicable in member states, i.e. it does not require separate implementing legislation. Under the GDPR, member state data protection authorities will be responsible for enforcement and the consistency of enforcement across the EU will be the responsibility of the newly created European Data Protection Board. Moreover, violations of the GDPR can lead to fines of up to 4 percent of total worldwide annual turnover (GDPR Article 83).

This section will focus on the GDPR since it will be the relevant law from May 2018. Where pertinent, this section will identify how the GDPR changes the scope and application of the Directive to give a better sense of the impact of the GDPR on digital trade.

What Are Personal Data?

The Directive defines personal data as "any information relating to an identified or identifiable natural person", and defines an identifiable person as "one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more specific factors specific to his physical, physiological, mental, economic, cultural or social identity" (Directive Article 2). The GDPR adopts a similar approach. It defines personal data as the Directive does, but widens the definition of an identifiable natural person to "one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identify of that natural person" (GDPR Article 4.1).

The main categories and areas of collection of personal data have been identified as (World Economic Forum 2014):

- data volunteered or created by individuals online such as through online registration, ecommerce transactions, social networks, emails, tweets;
- data observed from internet browsing, and location data from smart phones; and
- data used to infer a personal profile from a range of data, some of which is personal data and some of which is non-personal data, but when synthesized and analyzed can produce a personal profile.

As this taxonomy reveals, distinguishing between personal data and non-personal data is not straightforward. For instance, collecting data on habits, locations and physical conditions may, over time create a personal profile of a person, even if each individual bit of data collected is not personal (USFTC 2015).

The Controller and the Processor of Personal Data

The approach in the Data Directive and the GPDR to protecting privacy is based on a framework that breaks down data and data processing (online and offline) into data subjects, controllers, and regulators. The GDPR defines a controller as "…the natural or legal person, public authority, agency or other body which alone or jointly with others determines the purposes and means of the processing of personal data". A processor is defined as "…a natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller" (GDPR Article 4.8). Whereas a controller is able to control the collection and processing of data, a processor processes data under instructions from the controller.

Key Privacy Commitments

The GDPR lists five principles that govern the processing of personal data. These are essentially good practices for handling personal information. These principles require that personal data are (Directive Article 5):

- processed fairly and lawfully;
- collected for specific, explicit and legitimate purpose and not further processed in a way incompatible with those purposes;
- adequate, relevant and not excessive in relation to the purposes for which they are collected
- accurate and where necessary, kept up to date; and
- kept in a form that permits identification of the data subject for no longer than is necessary for the purpose for which the data were collected.

The GDPR also gives a data subject a range of rights, the main ones being a right to information on the personal data being held by a controller, including how it is stored, the right to rectification (the so-called right to be forgotten) and a right to the erasure of personal data (GDPR Articles 15-20).

The GDPR allows for processing personal data only under specific circumstances. The main ones are where: the data subject has unambiguously given consent; processing is necessary for the performance of a contract to which the data subject is a party, for compliance with a legal obligation to which the controller is subject, to protect the vital interests of the data subject, or it is in the public interest.

Processing is also allowed for the purposes of the legitimate interests pursued by the controller, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject (GDPR Article 6).

The Territorial Scope of EU Data Privacy Laws

The Directive requires Member States to apply their data privacy laws to third parties not located in the EU in two circumstances. First, where the "processing is carried out in the context of the activities of an establishment of the controller in the territory of a Member States" (Directive Article 4.1.a). Second, where "the controller is not established on Community territory and, for purposes of processing personal information makes use of equipment, automated or otherwise, situated on the territory of the said Member State" (Directive Article 4.1a). What constitutes "processing…in the context of activities of a controller" was addressed by the Court of Justice of the European Union, which found that even though Google was collecting and processing data in the United States, the activities of its subsidiary in Spain that sold advertising was "in the context of activities of a controller", thereby bringing Google's processing of personal data within the jurisdiction of the Data Directive (Google Inc v. Agencia Espanola de Proteccion de Datos 2014).

The GDPR avoids the Directive's reference to "use of equipment" in a member state to ground jurisdiction. Instead, jurisdiction extends to the following: 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 take places in the EU or not; the processing of personal data of data subjects who are in the Union by a controller or a processor not established in the Union, where the processing of activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behavior as far as their behavior takes place within the Union (GDPR Article 3). Where the controller is not based in the EU, then the Regulation, like the Directive, requires that the controller designate a representative in the Union (Regulation Article 27).[3]

The emphasis in the GDPR on whether the Controller offers goods and services or monitors behavior rather than whether it uses equipment, focuses on the type of activity that can give rise to privacy concerns. For instance, offering of goods or services captures how online commerce leads to the collection of personal data, such as when a name, address and bank account details are used to finalize the online purchase (Schwartz 2013). Recital 23 of the GDPR provides additional context, noting that mere accessibility of a website in the EU may not be enough to bring that entity within the Regulation, but combined with use of an EU member's language and with opportunities to purchase is likely to constitute an offering for sale under the GDPR.

The second type of personal data collection covered by the GDPR - monitoring the behavior of data subjects - includes internet use that is not directly commercial or transactional, such as monitoring internet search behavior. Recital 24 of the Regulation elaborates on the meaning of "monitoring" as occurring when "individuals are tracked on the internet with data processing techniques which consist of "profiling" a person, particularly in order to take decisions concerning her or him or for analyzing or

[3] However, the Regulation does not require an EU representative when the controller (a) is in a third country with an adequate level of protection; (b) is an enterprise employing fewer than 250 persons; (c) is a public authority or body; or only occasionally offers goods or service to data subjects in the EU.

predicting her or his preference, behaviors or attitudes." Taken together, this would appear to capture a large amount of what happens when people use the internet.

Transferring Data from the EU to Third Countries

Under the Data Directive and GDPR, data can be transferred outside the EU under various conditions. The main one is where the European Commission has found that the third country receiving the personal data provides an adequate level of protection (GDPR Article 45). In the absence of an adequacy decision, the GDPR allows data to be transferred outside the EU pursuant to various safeguards or a derogation – the main one being explicit consent (GDPR Article 44).

Adequacy Findings

The Directive requires an adequacy assessment to be based on "all the circumstances surrounding a data transfer" with particular attention to the following factors: nature of the data, the purpose and duration of the proposed processing, the country of origin and country of final destination, the rule of law and the professional rules and security measures complied with.

The GDPR also requires an adequacy finding and provides a more comprehensive list of the considerations in an adequacy finding and which largely reflect the Article 29 Working Party approach (Regulation Article 41.1-2). These include the existence of the rule of law; legislation including public security, national security, criminal law; whether there are effectively enforceable rights including administrative and judicial redress for data subjects; and any international commitments entered into by the third country (GDPR Article 45.2).

The GDPR also allows the Commission to make an adequacy finding with respect to a territory or one or more sectors within a third country, or an international organization (Regulation Article 45.3). This would seem to open the door for the Commission to find that specific states or economic sectors within a country provide an adequate level of protection. This provision would cover the US-EU Privacy Shield**,** which only applies to specific economic sectors and is discussed below.

So far, outside Europe and British territories in Europe, only five countries have received a national adequacy finding (Argentina, Uruguay, Israel, New Zealand, and Canada (commercial organizations)).[4] While in determining adequacy, the Directive allows for consideration of alternatives to top-down legislated approaches to privacy regulation such as industry self-regulation, the countries mentioned were found to have adequate privacy protection based on specific economy-wide laws. For instance, Argentina and Uruguay were assessed as providing an adequate level of data protection based on their constitutional provisions and other legislation (EC 2003).

In practice, the EU approach to privacy requires other countries to have in place a privacy regime that is essentially equivalent to the EU (Schrems v. Data Protection Commissioner 2015). This equivalence relates not only to the level of data protection but also to whether the access of government agencies to personal data and data subjects' rights of redress are consistent with the GDPR.

[4] The EU-US Privacy Shield is not a finding of national adequacy but a finding that the Privacy Shield per se provides adequate protection (European Commission 2017; Official Journal of the European Union 2000, 2001, 2011, 2012, 2013, and 2016).

Notwithstanding the limited number of adequacy findings to date, the Directive has become a reference for other countries as they developed their own privacy laws. According to one study analyzing the impact of the Directive on the development of other countries' privacy regimes, of the 39 countries outside Europe with data protection laws adopted after the Directive, 13 are highly similar to the Data Directive and another 19 are very similar (Greenleaf 2012). This group includes countries such as Peru; Colombia; the Republic of Korea; Taiwan, China; and Hong Kong SAR, China.

Transfers subject to safeguards

In the absence of an adequacy finding, the GDPR provides a number of mechanisms for transferring personal data to another jurisdiction (GDPR Article 46). Each mechanism needs approval by either the Commission or a member state privacy authority. The main ones are binding corporate rules, contract, an approved code of conduct, and an approved certification mechanism.

Binding Corporate Rules (BCRs) were designed in response to the need for multinational companies to move data globally. The GDPR defines BCRs as personal data protection policies consistent with the GDPR and which are adhered to by a controller or processor established in the territory of a member state for transfers of personal data to a controller or processor in one or more third countries within a single conglomerate or within a group of enterprises engaged in a joint economic activity (Article 47). The GDPR requires that BCRs are legally applied and confer enforceable rights on data subjects (Article 47.2). In addition, to establish a BCR, the GDPR requires a controller or processor to be established in a Member State who can be held liable for breach (Article 47.2f).

Standard Contractual Clauses (SCCs) are encouraged by the Directive, presumably to help streamline and simplify the process of data transfer. According to an Article 29 Working Group opinion, such contracts will require the same levels of protection, oversight and access for individuals as would be the case with an adequacy decision. The GDPR continues the use of contract as a means for transferring personal data outside the EU.

Codes of Conduct can apply to associations representing controllers or processors and can be used to ensure compliance with the GDPR privacy standards (GDR Article 40-41). Any code must be approved by the Commission and be subject to monitoring and enforcement by an accredited entity within an EU member state.

Approval Certification Mechanisms, provided for in the GDPR, allow the development of data protection seals and marks to demonstrate compliance with the GDPR by processors and controllers within the EU. These codes can also be used by businesses outside of the EU and where approved, can serve as a basis for transferring personal data outside the EU (GDPR Article 42).

Codes and certification mechanisms are new under the GDPR. The Commission has flagged interest in developing these mechanisms to maximize opportunities for cross-border data flows (EC 2017a). However, the approach of the Court of Justice of the European Union is likely to limit the potential scope for such mechanisms.

Limits to safeguards for transferring data out of the EU

Each of the safeguard mechanisms for the transfer of data have their limitations. BCRs tend to be used by large companies as their main mechanism for transferring personal data outside the EU but within the conglomerate. BCRs involve a lengthy implementation and approval process from Data Protection Authorities. The extension under the GDPR of BCRs to enterprises engaged in a joint economic activity increases flexibility. However, BCRS are still unlikely to be available for small business seeking to export digital services to the EU. Contracts have also proved unwieldy as they must be designed to deal with all possible data transfers, and therefore are unable to respond to data transfer needs without having to amend the contract. It remains to be seen how the codes of conduct and certification schemes operate under the GDPR. Yet, the key point remains that under all the safeguard mechanisms, the GDPR requires demonstration of compliance with GDPR standards, rights of data subjects and enforcement mechanisms.

The case involving the *Irish Data Protection Authority and Facebook Ireland Inc. and Schrems* has also called into question the extent to which contracts are available in the absence of an adequacy finding. In that case, the Irish High Court agreed with the assessment of the Irish Data Protection Authority that notwithstanding the EU Commission adequacy finding with respect to Privacy Shield, the United States fails to provide EU citizens with access to legal redress in case of misuse of personal data consistent with the requirement of Article 47 of the European Charter of Human Rights. Of significance for future use of contracts (the reasoning is also applicable to BCRs) is the finding that key issues such as how a third-country government accesses personal data for national security purposes is fundamental to whether contracts protect EU personal data consistent with the GDPR. This highlights a key limitation of contracts (and BCRs) – that these mechanisms do not bind the government in the data-receiving country. As a result, even where such arrangements bind private parties to protect data consistent with the GDPR, if the broader privacy regime in the third country is also not consistent with the GDPR then contracts (and BCRs) are also likely to be unavailable. The net effect is that in practice under the GDPR, in order to use contracts and BCRs will require the data-receiving country to have in place a privacy regime that, at least in terms of availability of oversight and redress mechanisms, could pass an adequacy finding. This case has now been referred to the CJEU.

Derogations

A Controller can also rely on so-called derogations. Under the GDPR, the main ones are: consent by the data subject, transfers necessary for the performance of a contract between the data subject and the controller, or transfers necessary for the purposes of a legitimate interest pursued by the controller, which cannot be qualified as frequent or massive (Directive Article 7f and Regulation Article 49.1h).

None of these derogations has proven suitable for businesses collecting and transferring personal data outside the EU. For instance, under the Data Directive, for *consent* to be effective to authorize cross-border data transfers it must be "specific and informed". The GDPR goes a step further and requires explicit consent to the proposed transfer "after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards" (GDPR Article 49.1a).

There are also limits to necessity for *performance of a contract* as a basis for data transfer. In many cases, the controller will not have a contract with a data subject. For instance, collecting and processing personal data from internet use i.e. "monitoring", would not create a contractual relationship. Even where a contract existed, the data transfer must be "necessary" for the performance of the contract. This would include transferring financial and personal information to complete an online

transaction. However, collecting other data incidental to the transaction such as on consumer preferences for goods and services would not appear to be necessary for the performance of the contract and therefore unlikely to justify data transfers outside the EU.

The ability to transfer data outside the EU *pursuant to a legitimate interest* is heavily circumscribed. First, the data transfer must not be frequent or massive, and so this derogation could not be used to justify an online business that relies on regular data collection. Where businesses seek to use this derogation for more limited data transfers, they must demonstrate that they have put in place appropriate safeguards to protect the data, to assess and provide suitable safeguards and to inform the EU supervisory authority of the transfer of data.

III. THE IMPACT OF EU PRIVACY REGULATION ON EXPORTERS: THE EXAMPLE OF INDIA

It is useful to demonstrate how the EU assesses adequacy in practice, focusing on India. The country's experience is relevant for a number of reasons. India is in the process of developing privacy regulation. India is also a developing country with significant services exports to the EU that rely on cross-border data flows, and so the economic and trade impacts of the Data Directive and GDPR could be significant.

India's Personal Information Protection Regime

As noted above, countries approach the issue of privacy protection differently, in part because of the historically contingent nature of privacy. In India, an emphasis on community norms and other post-colonial priorities meant that individual rights to privacy have developed incrementally through common law or court made decisions. Initially, the Supreme Court recognized the constitutional right to privacy and stated that this right needs to be balanced against the constitutional right to free speech (*R. Rajagopal v. State of Tamil Nadu 1994*).

India has various legislative and judicial protections applicable to personal information. The Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules) incorporate some of the OECD privacy principles such as collection limitation, use limitation and individual participation. They require collection of personal information for lawful purpose connected with the function of the business and require consent of the individual prior to disclosure. The SPDI rules only apply to corporate entities and cover 'sensitive personal data' such as sexual orientation and medical records and not the larger range of personal data. More recently, the Aadhaar Act 2016 enables the government to collect personal information and to issue a unique identification number. Collection of these data is to be done consistent with various data protection principles including ensuring security and confidentially.

The Aadhaar Act was subject to challenge before the Indian Supreme Court (*KS Puttaswamy v. Union of India 2017*). In that case, privacy advocates had challenged the "Aadhaar" scheme. The concern was that the collection of biometric data associated with the card, and the links to bank accounts and mobile telephones, was intrusive. The court ruled that there is a right to privacy in India, based on the Constitution's right to life and personal liberty in Article 21 and all fundamental rights in Part III of the Constitution. The Court also recognized that this right or privacy is not absolute and subject to reasonable restrictions.

The court reserved judgment on the constitutionality of the Aadhaar scheme, which will be determined by another bench of the court but said, "In an age where information technology governs virtually every aspect of our lives, the task before the Court is to impart constitutional meaning to individual liberty in an interconnected world. While we revisit the question whether our constitution protects privacy as an elemental principle, the Court has to be sensitive to the needs of and the opportunities and dangers posed to liberty in a digital world…Since the government has initiated the process of reviewing the entire area of data protection, it would be appropriate to leave the matter for expert determination so that a robust regime for the protection of data is put into place."

The Indian government is in the process of further developing privacy legislation. Towards this end, the government has convened a group of experts to study the issue. The government has stated that the objective is to "ensure growth of the digital economy while keeping personal data of citizens secure and protected." A White Paper has been drafted and public comment were solicited to help shape development of the law. The questions posed in the White Paper suggest that an adequacy requirement – possibly modeled on the EU approach – is being considered to govern cross-border transfer of personal information.

India's services exports to the EU

The internet and the ability to move data freely and globally are an increasingly important driver of India's services exports (Mattoo and Wunsch 2004). Over 40 percent of all goods and services exports consist of software services (which includes information technology (IT) services and software product development) and information technology enabled services (ITES). The latter include financial analysis, accounting, medical transcription, social networks, online gaming, the provision of apps for smartphones and online services for the health care industry. For example, AdventNet in Chennai operates popular web-based applications that are used in hospitals, and Healthcare Offshoring provides medical transcriptions, billing and insurance, claims, tele-imaging and telepathology (Kshetri 2010).

Cloud-based services are another key area of growth and opportunity for India's internet enabled services sector exports. In this regard, companies are building data centers to provide cloud-based services globally. For example, IBM has established a cloud center in Bangalore, Salesforce offers a cloud service focused on software and Microsoft has a cloud in India that offers Business Productivity and Office Suite with email, live meeting and collaboration tools. Additionally, cloud services are opening up new opportunities for R&D collaboration globally. For example, India's Computation Research Laboratories is a cloud provider that allows for research with other entities in India and globally.

Cross-border data flows are, therefore, vital for India's exports of services and Europe is an important destination. About two-thirds of India's IT and IT-enabled exports are delivered cross-border and only about one-third through a commercial presence or the presence of an Indian individual (Reserve Bank of India 2017). Virtually all of these cross-border exports tend to be provided online and are reliant on international data flows (Eichengreen and Gupta 2010). About 23 percent of India's IT and IT-enabled exports went to Europe in 2016-17, making it the third largest destination for such exports from India, after the United States and Canada. Provision of these services often requires the collection of data from EU citizens and is therefore affected by the EU's privacy laws.

The EU White Paper on India

In 2010, the EU commissioned a White Paper to assess the adequacy of the protection of personal data in India (Greenleaf et al 2010). The report concluded that India did not provide an adequate level of privacy protection. While the Report recognized that there was a constitutional right to privacy in India, it determined that the right fell short of providing adequate protection, as it did not comprehensively apply to data collected by the private sector. Other important concerns in the report were the limited focus of India's main privacy legislation on cybersecurity, inadequate opportunities for data subjects to enforce rights to access and rectify data held by private companies, no laws limiting the transfer of personal data outside of India, the failure to extend the right of access to information to non-citizens in India, and the absence of protections from direct marketing (Greenleaf et al 2010). The Report also emphasized the lack of compliance and limited ability of enforcement mechanisms in India to deliver compliance. There was no assessment of what would be an appropriate level of compliance for India given resource constraints and other competing priorities.

This white paper highlights a disconnect between the EU's internal approach to privacy, which is characterized by low levels of compliance and a balancing of privacy interests, and its approach to privacy rules in other countries. For example, former EU Ambassador to India Joao Cravinho was quoted as saying that "data protection is our fundamental right and rights are not negotiated" (Basu 2013). If this is indeed the position, it fails to recognize that within the EU Directive and GDPR, the right to privacy is balanced against other goals, such as national security. Most recently the Irish High Court, in assessing the use of standard contractual clauses under the Data Directive to transfer personal data from the EU to a country without an adequacy finding, notes that a balance must be struck between these competing concerns, interests and values – in this case the right to privacy and national security needs, and that "not every State will strike the same balance" (Irish High Court 2016).

This example suggests that the EU approach to the Directive's requirement of adequacy leverages access to the EU market to induce other countries to adopt data protection regimes equivalent to the EU even though it may not be optimal for them in economic and broader social terms. A privacy regime equivalent to the EU regime in terms of substance and enforcement would fail to recognize India's own legal, cultural, and historical trajectory.

As outlined, EU history and development of privacy as a fundamental human right has led to a particular balancing of privacy protection and economic and trade opportunities. The Commission claims that strong privacy protection gives companies a competitive advantage – suggesting a false choice between privacy and realizing the economic and trade opportunities from data flows (EC 2017a). Competitive advantage is most likely in markets where consumers are sensitive to privacy, but the high costs of compliance are likely to lead to a loss of competitiveness in other markets. One study estimated that the GDPR's impact on data flows will reduce EU GDP by 0.4 percent and more severe disruptions to the flow of personal data could reduce EU GDP by over 1 percent (Bauer et al 2014).

As a developing country, India's approach to privacy may strike a different balance between managing the risks that use of personal data could result in a breach of privacy with the economic and trade potential of such data use. Furthermore, in a developing country with one-fifth of the population below the poverty line, India's thriving IT industry and export-orientated businesses present an important opportunity to engage in sophisticated services trade and stimulate economic growth. How India balances these development needs, economic opportunities from the internet and privacy goals will reflect these dynamics.

One more reason why the EU approach to data privacy might not be optimal for India is the use of consent as a basis for processing personal data. The increasing capacity to aggregate and process data means that even when a particular piece of data is not personal, the collection and compiling of such data can build a complete personal profile. To determine when consent to processing will turn data into personal data in this context is particularly challenging. In addition, obtaining informed consent in India from a large population with relatively low literacy rates is not only practically challenging, but also may not be meaningful even when it is obtained.

Access to other Mechanisms for Cross-Border Data Transfers

In the absence of an adequacy finding, Indian companies can seek to use BCRs and SCCs. But in that case, the Data Directive and Regulation create a strong incentive to establish a local presence because access to both BCRs and SCCs requires a controller located in the EU. Many of the opportunities for India's IT services exports are in providing internet-based services from India, either on an outsourcing or contract basis, to companies and increasingly directly to consumers in the EU. In the majority of cases, Indian firms do not have a commercial presence in the EU. The biggest benefit of the internet for SMEs and developing countries is the ability to avoid having to establish a commercial presence in another country that could involve relatively significant costs and reduce some of the benefits of the internet for international trade.

The impact of EU Privacy Regulation

The efforts by some developing countries (most clearly the Philippines and, to an extent, India) to respond to the EU privacy directive illustrates the dilemma for developing countries. The solutions on offer, adequacy of national privacy protection, binding corporate rules and model contracts, present countries with a trade-off. A key issue is that in the case of national adequacy findings, privacy standards are not "separable," i.e. must be met for sales to all markets, rather than separable by destinations, like model contracts.

On the one hand, if they chose to enact a national law deemed adequate, individual firms are spared the need to incur any EU-specific costs associated with BCRs and SMCs. However, a national law would require all firms to adhere to the same stringent privacy standard regardless of which foreign or domestic market they serve. The result could be an economy-wide increase in the costs of doing business. In fact, the Philippines initially enacted national privacy legislation to ensure continued access to the EU data processing market. However, the result was that many Philippines-based US firms found it difficult and costly to operate in the Philippines and suspended investment plans, whereupon the Philippines government was obliged to reversed course.[5]

On the other hand, if they do not enact a national law deemed adequate, firms would be required to ensure privacy protection either through BCRs or SCCs. In the case of the latter, firms would retain the flexibility of adhering to different privacy standards on their operation in other markets. The former would imply a loss of flexibility for that specific firm but continued flexibility for other firms in that country. Both routes are likely to be time-consuming and costly (see below). Furthermore, in the absence of such laws, and given the weakness of local legal and regulatory systems, it might be difficult

[5] Fifteen Congress of the Republic of the Philippines (2011), Senate Committee Report No. 56, Re: Senate Bill No. 2965.

for private firms in developing countries to emulate U.S. firms like Microsoft and credibly commit to meet the required high standards (see the discussion of the EU-US Privacy Shield).

A NASSCOM-DSCI Survey in 2013 suggested that the EU regulation had a significant impact on India's exports (NASSCOM-DSCI 2013).[6] The respondents accounted for about 45 percent of industry revenues, and spanned IT (e.g. custom application development) and BPO (e.g. customer care, finance and accounting, human resources) sectors. As many as 90 percent of the respondents said they used standard model contracts to transfer personal data outside the EU. Most said that the process was complex and lengthy; more than half said it took on average more than 3 months. A small number said they used binding corporate rules and indicated that the process took over 6 months. As many as 67 percent of the surveyed services exporters claimed "non-fructification" of deals because of data protection-related concerns. Nearly, two-fifths of respondents estimated a loss in commercial opportunities of more than $10 million and another one-third of between $1 million and $10 million.

IV. THE TREATMENT OF PRIVACY UNDER CURRENT AND PROPOSED TRADE RULES

In this section, we briefly review how privacy is treated under the rules of three representative trade agreements: the WTO, the Korea-US Free Trade Agreement and the CPTPP.

The WTO

The WTO rules that affect data flows are contained in the General Agreement on Trade in Services (GATS). Four aspects the GATS rules are relevant: the coverage of digital flows under the GATS; the substantive disciplines on openness; the exceptions provisions pertaining to privacy; and the provision relating to recognition agreements.

The coverage of digital flows under the GATS

The Appellate Body has confirmed that specific commitments on services include their electronic delivery (WTO 2012, para 364). This is consistent with the view that specific commitments are "technologically neutral." Therefore, a commitment to allow the cross-border delivery of a service can be assumed to mean that delivery through all means – including as digital flows – is allowed. However, this commitment does not extend to requiring unrestricted flows of personal data. For example, a commitment to allow the cross-border supply of life insurance services does not necessarily oblige a country to allow an insurer located abroad to transfer personal health data out of the country.

There is some uncertainty about the extent to which *new* digital services are covered by existing GATS commitments. Most WTO members used the UN Central Product Classification (CPC) System or the Services Sectoral Classifications List (MTN/GNS/W/120) (or a combination of both) to schedule their WTO GATS commitments. The CPC was finalized in 1991 when the internet barely existed. The CPC has since been updated but the older CPC classification remains the basis for members' GATS commitments. The most relevant CPC for digital services are CPC 843 for 'computer and related services', and CPC 844 for 'Data Base Services' which includes online processing services. Yet, it is open to question whether these classifications cover 'new' digital services such as search engines and cloud computing which did not even exist when commitments were scheduled.

[6] These data have not been independently verified.

The Understanding on Financial Services, which has been used by a subset of WTO members to schedule commitments in financial services contains an explicit provision to allow "Transfers of Information and Processing of Information." It states that "No Member shall take measures that prevent transfers of information or the processing of financial information, including transfers of data by electronic means … where such transfers of information, processing of financial information … are necessary for the conduct of the ordinary business of a financial service supplier."

Substantive GATS disciplines on openness

The three pillars of the GATS are the provisions on Most-Favored-Nation (MFN) Treatment (Article II), National Treatment (Article XVII) and Market Access (Article XVI). These provisions seek to prevent discrimination between trading partners, discrimination in favor of domestic providers, and the use of specific quantitative restrictions. MFN and National Treatment cover in principle both de jure and de facto discrimination, i.e. both explicitly different treatment and effectively different treatment. The market access (Article XVI) obligation differs from the other two provisions in that it prohibits only de jure quotas but not de facto quotas. The limitations of the key GATS disciplines are well recognized. For example, the National Treatment and Market Access obligations apply only in sectors included in a WTO Member's schedule and there too can be subject to limitations.

Most WTO members have made limited specific commitments offering national treatment and market access on cross-border trade, choosing to be relatively open in areas like computer services but relatively cautious in areas like banking, insurance and regulated professional services (Mattoo and Wunsch, 2004). In the absence of such commitments, a member is under no obligation to allow the related flows of data. However, the EU and many other countries' commitments on computer related services and database services state there are no restrictions on market access or national treatment (WTO 1994). This liberal attitude may reflect, as noted above, that governments prepared their GATS commitments in the late early 1990s, when cross-border digital delivery of search, audiovisual, cloud computing, and other services had not assumed the scale that exists today.

The GATS exceptions provisions pertaining to privacy

GATS commitments co-exist with an exceptions provision (Article XIV(c)). The exceptions provision allows WTO members, inter alia, to take measures necessary to prevent deception and fraud and protect the privacy of individuals. But such measures must comply with the chapeau of Article XIV – that the measure is not applied in a manner that leads to arbitrary or unjustifiable discrimination or a disguised restriction on trade in services.[7]

The WTO Appellate Body has found that whether a measure is 'necessary' requires "weighing or balancing" factors including the contribution of the measure to the policy goal, the importance of the common interests or values protected by the measure as well as the impact on imports (WTO 2007). This includes assessment of whether there is a less restrictive alternative measure that could achieve the WTO member's goal – in this case the protection of individual privacy. Here, the Appellate

[7] The provision Understanding on Financial Services also includes an exceptions clause, which states that "Nothing in this paragraph restricts the right of a Member to protect personal data, personal privacy and the confidentiality of individual records and accounts so long as such right is not used to circumvent the provisions of the Agreement" (Understanding on commitments in financial services 1995, Article b8).

Body has found that "to qualify as a genuine alternative", the proposed measure must not only be less trade restrictive than the original measure at issue, but should also "preserve for the responding member its right to achieve tis desired level of protection with respect to the objective pursued" (WTO 2014). Assessment of the consistency of a measure with the GATS Article XIV chapeau is about "locating and marking out a line of equilibrium between the right of a Member to invoke an exception under Article *GATS Article XIV* and the rights of other Members under varying substantive provisions" (WTO 2001, para 159). A cooperative process involving WTO members rather than a WTO dispute settlement panel may be a more reliable process of finding such a "line of equilibrium."

The provision relating to recognition agreements

GATS Article VII on mutual recognition provides an avenue to develop interoperability among privacy regimes. On the one hand, it is permissive and allows space for regulatory cooperation. Thus, Article VII:1 recognizes that "For the purposes of the fulfilment, in whole or in part, of its standards or criteria for the authorization, licensing or certification of services suppliers, … a member may recognize the education or experience obtained, requirements met, or licenses or certifications granted in a particular country" as part of an agreement or autonomously.

On the other hand, Article VII seeks to ensure that this freedom is not abused. Article VII:2 requires a Member who enters into a mutual recognition agreement (MRA) to afford adequate opportunity to other interested Members to negotiate their accession to such an agreement or to negotiate comparable ones. For instance, once the EU recognized the US conformity assessment procedures under the Privacy Shield (see below), it would be obliged to grant other countries also an adequate opportunity to negotiate a similar arrangement.[8]

More importantly, Article VII:3 stipulates that a Member must not grant recognition in a manner which would constitute a means of discrimination between countries in the application of its standards or criteria for the authorization, licensing or certification of services suppliers, or a disguised restriction on trade in services. Recognition, unilateral or through an MRA, amounts to an acceptance of likeness vis-à-vis certain suppliers. It also defines a standard of treatment vis-à-vis other suppliers and provides others with a potentially valuable foothold. Article VII offers potentially valuable mechanisms for broadening bilateral initiatives, as we discuss below.

Korea-US FTA

This agreement took an important first step in explicitly covering data flows in its Chapter 15 on Electronic Commerce. But since the approach was much more fully developed in the subsequent CPTPP, which dealt with privacy explicitly and substantively, we consider the provisions of the Korea-US FTA only briefly.

Essentially, the agreement balances a soft provision on allowing data flows with an even softer provision on consumer protection rather than ON privacy per se. Article 15.8 contains a "best endeavor"

[8] The requirement in GATS Article XIV chapeau that measures not be applied in a manner that constitutes arbitrary discrimination could also create a similar obligation (see the discussion of the shrimp-turtle case in Howse 2002, 505).

obligation on Parties "to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders" while "acknowledging the importance of protecting personal information." This provision is complemented by Article 15.5 on Online Consumer Protection which states that Parties to the agreement "recognize the importance" of measures to protect consumers from fraud and of cooperation between their respective national consumer protection agencies which they shall endeavor to do.

Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP)

What was originally the TPP provision and eventually became the CPTPP provision on data flows, contained in Chapter 14 on Electronic Commerce, has been widely and justifiably described as far-reaching. As the USTR website stated, before the United States withdrew from the agreement, the "TPP will help preserve the open internet and prevent its breakup into multiple, balkanized networks in which data flows are more expensive and more frequently blocked." The CPTPP provides a multi-tiered approach to enabling cross-border data flows and developing the interoperability of privacy protection regulations.

The first key development in the CPTPP is the explicit obligation under Article 14.11.2 that "Each Party shall allow the cross-border transfer of information by electronic means, including personal information, when this activity is for the conduct of the business of a covered person." These commitments cover all information flows and, unlike the GATS, are not limited to data flows necessary for the provision of cross-border services. Similarly, even though data localization requirements could arguably fall foul of the GATS national treatment obligation because they could be regarded as de-facto discriminatory, it helps to have an explicit obligation in Article 14.13.2 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."

The CPTPP also includes an exceptions chapter like GATS Article XIV in its electronic commerce chapter. In addition, the same article containing the commitment to cross-border data flows includes an exception for measures "to achieve any legitimate public policy objective, provided the measure is not applied in a manner that would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on and trade; and does not impose restrictions on transfers of information greater than are required to achieve the objective" (CPTPP article 14.11.3). While this exceptions provision too largely reflects GATS Article XIV, the extension to all legitimate policy objectives reflects concern as to the potentially limited scope of public policy measures that could fit within the GATS exception.

Thus, the CPTPP approach to privacy pairs a commitment to data flows with scope for parties to restrict flows of personal information where needed for legitimate policy reasons, including personal privacy protection. In practice, it also means that where cross-border data flows could undermine achieving domestic privacy goals, then the CPTPP provides ample scope for such data flows to be restricted. In the absence of mechanisms that ensure agreed standards for privacy protection, we would expect heavy reliance on such an exceptions provision to limit transfers of personal data.

This is where the CPTPP includes another important development by creating *obligations on data destination countries* to prevent fraud and deception and to protect personal information. Thus, Article 14.7.2 on Online Consumer Protection requires that "Each Party shall adopt or maintain consumer protection laws to proscribe fraudulent and deceptive commercial activities that cause harm or potential harm to consumers engaged in online commercial activities." Article 14.8.2 on Personal

Information Protection requires that "each Party shall adopt or maintain a legal framework that provides for the protection of the personal information of the users of electronic commerce." In addition, Article 14.8.3 stipulates, "Each Party shall endeavor to adopt non-discriminatory practices in protecting users of electronic commerce from personal information protection violations occurring within its jurisdiction." Finally, Article 14.7.3 encourages cooperation in this respect between national consumer protection agencies and 14.8.5 encourages the development of mechanisms to promote compatibility between different regimes for protecting personal information.

Such obligations on data destination countries are a key element of the cooperation that is needed to reassure data source countries that their commitments to cross-border data flows will not place their consumers or broader regulatory needs at the mercy of indifferent foreign regulators. Moreover, the existence of such shared obligations also reduces the need for unilateral action by source countries under the exceptions provisions and, therefore, creates greater security of access to personal data for exporters. It remains to be seen how parties will interpret and implement the Article 14.8.3 stipulation to "endeavor to adopt non-discriminatory practices in protecting users of electronic commerce," and whether all consumers and contracts will be adequately covered regardless of the jurisdiction in which they are located. Nevertheless, the CPTPP approach to data flows may well be a model for the form of regulatory cooperation that would induce wider and deeper commitments in services trade.

The close link between unrestricted data flows and regulatory cooperation was also evident in the decision to exempt the financial services industry from the CPTPP rules safeguarding the cross-border flow of data. Treasury Secretary Jacob Lew was reported to have defended the US insistence on this exclusion, stating, "One of the issues here is the requirements of our regulators in terms of ... what they need to have their prudential reviews of financial institutions. We can't give away something that our financial regulators would need here in the United States" (Law 360 2016). In future negotiations, if countries were to promise to "extradite" data needed for prudential reviews to the concerned regulator, then there would be less need for local data storage and the exclusion of financial services from the data flow obligation.

The EU's Proposed Approach in its Trade Agreements with Other Countries

The issue of privacy has been a key concern for the EU when it comes to negotiating commitments to data flows in trade agreements. For instance, during the Trade in Services Agreement (TISA) negotiations and the US-EU Transatlantic Trade and Investment Partnership (TTIP) negotiations, the US demand for a commitment to the free flow of data was resisted by the EU out of fear that this could be inconsistent with the Data Directive.

Recently, the EU has attempted to reconcile the importance of data flows with its approach to privacy. The EU has recently put forward an approach to data flows in its agreements with third countries that combines strong commitments to allowing data flows with an exceptionally permissive exceptions provision. The EU text provides robust cross-border data flows commitments similar to those in CPTPP – namely that data flows "shall not be restricted between the Parties" by (i) requiring the use of local computing facilities; (ii) requiring the localization of data for storage or processing; (iii) prohibiting storage or processing in another party; or (iv) making the cross-border transfer of data contingent on the use of local computing facilities or other localization requirements.

However, the text also includes a broad exception that permits each party to "adopt and maintain the safeguards *it deems appropriate* to ensure the protections of personal data and privacy." This italicized text intends to create a self-judging exception as to what is needed to ensure privacy protection. This exception resembles the broad national security exception included in trade agreements, which are similarly self-judging. The proposed EU approach also stands in contrast to how the exception for privacy is dealt with in the GATS – which as outlined above, requires demonstration that the exception is "necessary" and complies with the chapeau requirement that the measure is non-discriminatory and least trade restrictive.

The Commission text goes even further and seems to carve-out rules and safeguards for the protection of personal data and privacy, including on cross-border transfers of personal data, from being part of the regulatory cooperation commitments in its FTAs. Given the importance of regulatory cooperation and the potential role for trade agreements to support progress here, such an approach is a missed opportunity.

V. INTERNATIONAL REGULATORY COOPERATION ON PRIVACY AND DATA FLOWS

In this section, we discuss two efforts at regulatory convergence, the OECD and APEC privacy guidelines and rules, respectively, and one effort at the recognition of conformity assessment procedures, the EU-US Safe Privacy Shield.

The OECD Privacy Guidelines

In 2013, the OECD released *Guidelines Governing the Protection of Privacy and Trans-Border Flows of Personal Data*. The Guidelines were produced in response to the significant changes in personal data collection since the rise of a global internet and the opportunities and risks of harm from online data collection and processing (OECD 2013). They are an update of the OECD's 1980 Privacy Guidelines and based on the Fair Information Practices Principles (FIPPS) developed in the United States. They also build on other OECD internet-related work such as the OECD Recommendation on Principles for Internet Policy Making 2011.

The Privacy Guidelines are a minimum set of principles governing the collection, storage and use of personal data to guide the development by Members of domestic privacy protection regimes. Many of these principles are reflected in the EU Data Directive, including:

- data are to be obtained by lawful means and where appropriate with the consent of the data subject;
- personal data should be accurate, complete and up-to-date;
- the purpose for collecting the data should be specified and the use of the data limited to fulfilling that purpose;
- personal data should not be disclosed within the consent of the data subject; and
- individuals have the right to obtain personal data from the data controller.

The Privacy Guidelines also expand on the so-called accountability principle as it applies to the data controller. Specifically, it requires the data controller to have in place a privacy management program that gives effect to these principles. The Guidelines require that privacy management programs are

tailored according to the sensitivity of the information and safeguards implemented based on a privacy risk assessment.

The Privacy Guidelines specify two ways in which data can be transferred across borders. One of these reflects the accountability approach where the data controller remains accountable for personal data under its control without regard to the location of the data. The other approach allows data flows to another country that "substantially observes the Guidelines" or where "sufficient safeguards exist", that would include mechanisms that ensure ongoing protection consistent with the Guidelines. According to the Supplementary explanatory memorandum to the Privacy Guidelines, these two principles on cross-border data transfer exist independently of each other (OECD 2013). These two approaches reflect the differing approaches among OECD members to cross-border transfers - the EU Directive and GDPR approaches, which limit transfers to countries providing adequate protection, and the APEC approach that allows data transfers and makes the data controller liable for any breaches of that data that arise for its use by third parties in other countries.

As outlined above, the OECD Privacy Guidelines also encourage "the development of international arrangement that promote interoperability among privacy frameworks that give practice effect to these Guidelines" (OECD 2013). How this might be accomplished is discussed below.

The Council of Europe Data Protection Convention and Additional Protocol

The European Council Data Protection Convention was adopted in 1980 (Council of Europe 1981) and its Additional Protocol in 2001 (Council of Europe 2001). Forty-three Council of Europe Member States have ratified the Data Convention and 42 Member States have signed the Additional Protocol (though only 31 have ratified the Protocol). The Convention and Additional Protocol are open to accession by non-EU states (The Convention, Article 23). The Council of Europe is also updating the Convention.

The key elements of the Convention are a set of privacy principles similar to those found in the 1980 OECD Guidelines, such as requiring personal data processing to be lawful, for specific and legitimate purposes and that it be adequate and not excessive in relation to the purposes for which the data are collected.

The Data Convention does not prohibit exports of personal data. This was changed following adoption of the Additional Protocol, which reflects the approach of the Data Directive and prohibits cross-border data flows unless the receiving country provides an adequate level of privacy protection.

Asia Pacific Economic Cooperation (APEC)

The APEC Privacy Framework endorsed by APEC economies in 2004 is a set of principles to guide members and businesses on privacy issues. The Framework is a guide for APEC economies on the development of their privacy laws, thus providing a baseline set of principles. APEC does not require or expect countries to adopt top-down privacy laws. Instead, the emphasis is on flexibility in implementation, which could include industry self-regulation in addition to legislation.

The APEC Framework is explicit about the need to "balance and promote both effective information privacy protection and the free flow of information in the Asia Pacific region" (APEC Privacy Framework 2004). The APEC Framework outlines the economic and social benefits of access to and storage of

information and expresses concern that regulatory systems that unnecessarily restrict or place burdens on data flows will have adverse implications for global businesses and economies.

The APEC Framework includes a set of information privacy principles similar to those found in the OECD Guidelines. These include:

- a need to protect the privacy of personal data according to the risks of harm from use and transfer of that data;
- notice to data subjects that personal information is being collected, the purposes for its collection, to which organizations the data might be disclosed and how the data subject can limit use and disclosure of the data, including opportunities to access and correct the data; and
- collection of data should also be limited to information for the purposes of the collection.

The APEC Framework departs from the OECD Guidelines and from the Directive in terms of the role of consent in the collection of data and when cross-border data transfers are allowed. For instance, consent or notice of the collection of data is only required "where appropriate." Additionally, data can be used for purposes other than the purpose of its collection with the consent of the data subject or where necessary to provide a service or product requested by the data subject.

Accountability is a key principle in the APEC Framework. It resides primarily with the business collecting the data to ensure that it complies with the APEC principles. This approach is similar to that in the Data Directive and GDPR use of contracts and BCRs to transfer data to third parties or within conglomerates (Article 29 Working Party and APEC 2005). But it does stand in contrast to the Data Directive's focus on whether countries have adequate privacy laws. And when transferring personal data to another person or organization whether in the same country or another jurisdiction, the person who collected the personal data is required to either obtain the consent of the data subject or to "exercise due diligence and take reasonable steps to ensure that the recipient person or organization will protect the information consistently with these Principles."

APEC Cross-Border Privacy Rules

The APEC Cross-Border Privacy Rules (CBPRs), endorsed by APEC in 2014 is a mechanism to facilitate the transfer of personal information amongst APEC members. The CBPRs were developed to address the key challenge outlined in this paper – how to facilitate transfers of personal data among countries with different privacy laws.

The CBPR requires business to develop privacy policies based on the APEC privacy principles and which meet the CBPR program requirements (CBPRs 2015). APEC Accountability Agents assess consistency of businesses privacy policy and practice with the APEC CBPR requirements. Businesses that meet the CBPR requirements and are subject to the laws of an APEC CBPR participating economy can then be certified as compliant. Currently, the United States, Mexico, Japan, Canada and Korea are participating economies and Australia and Singapore have announced plans to join. APEC Accountability Agents and Privacy Enforcement Authorities are responsible for enforcing compliance by business with APEC CBPR requirements.[9]

[9] See APEC Cross-Border Privacy Rules System, Policies, Rules and Guidelines, 10.

The E.U.-U.S. Privacy Shield

In 2016, the United States and the EU concluded the Privacy Shield – an arrangement that the EU Commission has deemed "adequate" under the Data Directive – thereby enabling the transfer of personal information from the EU to businesses in the United States participating in the Privacy Shield (EC 2016). The Privacy Shield replaced the EU-U.S. Safe Harbor framework, which in 2015 the CJEU found did not provide an adequate level of privacy protection due to an absence of rights of redress for EU citizens with respect to government access to their data (Schrems v. Data Protection Commissioner 2015).

Under the Privacy Shield, U.S. companies through an industry body or individually self-certify to the U.S. Department of Commerce that they will protect personal data consistent with the Privacy Framework, which includes the Privacy Shield Principles (Privacy Shield Framework 2018). These seven Principles (and supplemental principles) largely reflect the key elements of the EU Data Directive (U.S. Department of Commerce 2016). The mains ones are:

- To give European data subjects notice that a US entity is processing their data;
- To provide choice including whether to opt out of providing personal information;
- Accountability for any onward transfers to third parties of personal information;
- To take reasonable and appropriate steps to protect personal data from loss or misuse;
- To process personal data only for purposes the organization intends to use it;
- To give European data subjects access to their personal information and the ability to correct, amend or delete inaccurate information; and
- To enforce the principles and to give European data subjects access to affordable enforcement mechanisms.

U.S. businesses are required to publish their privacy policies, and the Privacy Shield gives the U.S. Federal Trade Commission jurisdiction over such businesses should they breach their own policy. In addition, the United States provides various means of redress for people, whose personal data has been compromised, including a direct complaint to the business or a complaint to the Department of Commerce. Also, under the Privacy Shield, the United States has agreed to establish an ombudsperson to address complaints about government agencies' access to personal information from the EU on national security grounds.

Despite the upgrading of privacy protection under the Privacy Shield compared with Safe Harbor, the stability of the arrangement is in doubt. The first annual review of the Privacy Shield by the Commission and the Department of Commerce identified a number of concerns on the EU side that the operation of the Privacy Shield is not providing a sufficient level of privacy protection. In particular, the EU expressed concern over inadequate access by Europeans to redress mechanisms, including failure to appoint officials at the State Department Ombudsperson (EC 2017).

VI. A PROPOSED APPROACH: BUILDING ON THE CPTPP AND THE PRIVACY SHIELD

Divergence in national privacy regulation is inevitable and even desirable, as discussed above. At the same time, developing global privacy principles can ensure a baseline of privacy protection and help to avert the negative impact of restrictions on cross-border data flows. Yet, even getting agreement on global privacy standards would not necessarily mean that such protection is extended to foreign citizens.

Simply pushing a traditional approach to trade rules, that only limits the data source country's freedom to regulate or prevent data outflows, fails to address the underlying problem in privacy regulation that leads to the need for data localization requirements in the first place. In fact, such commitments to cross-border data flows would merely lead to the data source country relying on the trade agreements exceptions for privacy measures to justify ongoing data restrictions. Such recourse to a trade agreements' exceptions provisions is implicit in the EU Commission proposal for balancing commitments to data flows with its privacy regime.

Under the circumstances, the most fruitful approach is to design trade rules, as in the recent Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), that reflect the bargain central to successful international regulatory cooperation, as in the EU-US Privacy Shield. Data destination countries would promise to protect the privacy of foreign citizens in return for source countries committing not to restrict the flow of data. While this goal may not be immediately attainable for a large group of countries, certain intermediate steps are likely to be feasible for different sets of countries.

Table 1 provides an overview of the different approaches to cross-border data flows of each privacy arrangement outlined in the paper. As can be seen, each of the privacy mechanisms relies on some convergence towards common privacy principles (whether in the EU or amongst a set of countries). As discussed, the CPTPP extends the scope of domestic privacy law to personal data collected from people located overseas. In this respect, the CPTPP resembles the Privacy Shield, which also extends US privacy protection to cover EU citizens. The table also shows that when it comes to enforcement of privacy principles, there are two broad approaches. In the first, entities collecting data and transferring it overseas remain liable and enforcement therefore happens in the data source country. In the second, cross-border transfers of personal data are subject to an adequacy finding or an international agreement which creates also an option of enforcement in the data destination country.

Table 1: Regulation of international transfers of personal information under different privacy regimes

	EU Data Directive/GDPR	**Privacy Shield**	**CPTPP**	**APEC CBPR**	**OECD Privacy Principles**
Privacy principles	Determined by the EU.	Determined by the EU, but recognition that US promise of privacy protection for EU citizens is equivalent to EU.	To be determined by each party, taking into account "principles and guidelines of relevant international bodies."	Common APEC privacy principles based on OECD – privacy floor which domestic privacy regimes can go beyond.	Common OECD privacy principles.
Scope	Applies to all companies collecting EU citizen data no matter where	Applies to US companies participating in Privacy Shield and collecting	Requires each Party to "endeavor to adopt non-discriminatory practices in protecting users of electronic commerce	Applies to APEC CBPR compliant[i] organizations. collecting personal	Applies to data controllers - entities who decide about the content and use of

	they are located.	data of EU citizens.	from personal information protection violations occurring within its jurisdiction."	information from APEC economies.	personal data, without regard to location of data.
Enforcement	National adequacy finding – data destination country enforces. BCR & SCC – data source EU country enforces against local entity.	US (data destination) country enforces; i.e. EU recognizes US enforcement procedures.	Unspecified. Depends on national privacy law.	Data source country by APEC Accountability Agent[ii] and Privacy Enforcement Authority (PEA)[iii], with cross-border enforcement cooperation facilitated by APEC Cross Border Privacy Arrangement.[iv]	Data source country enforcement against data controller.

[i] An entity is CBPR compliant when its self-assessment of compliance with its own data privacy policies against the APEC Privacy Framework has been reviewed by an APEC-recognized Accountability Agent.
[ii] An APEC Accountability Agent has met the APEC recognition criteria to the satisfaction of APEC economies.
[iii] A Privacy Enforcement Authority is any public body responsible for enforcing privacy law that can conduct investigations or pursue enforcement proceeding.
[iv] Endorsed by APEC Ministers in 2009, CPEA is a voluntary framework that aims to facilitate cooperation amongst PEAs in enforcing CBPR, such as parallel or joint investigations or enforcement actions. Information sharing and cooperation is also encouraged with privacy enforcement authorities outside of APEC.

This range of approaches to developing privacy principles, their scope and enforcement mean that a spectrum of options exist to access the economic opportunities from cross-border data flows while securing strong privacy protection. Action can range from unilateral action by source countries to mutually binding agreements between the source and destination countries. The location on this spectrum will depend on the degree of convergence between national privacy standards and extent of trust between national regulatory authorities.

i. *Unilateral action by data source countries*: At one end of the spectrum is the EU regime. Here, the data source country unilaterally sets its standards and determines whether destination countries comply with the standard. Furthermore, the source country retains complete discretion at each point of time in setting its standards.

ii. *Additional commitments by individual data source countries a la GATS Article XVIII*: As a first step in cooperation, the data source country may still specify conditions unilaterally and determine conformity unilaterally, but it may lend additional transparency and predictability to its requirements by listing them, e.g. as Additional Commitments under GATS Art. XVII. This provision is meant to house commitments of a regulatory nature that do not constitute limitations on either market access or national treatment. The Telecommunications Reference Paper – pertaining to

issues such as independence of regulators, licensing, interconnection and universal access – took the legal form of an additional commitment under the GATS. Even though WTO members negotiated a standard text for the Reference Paper, individual members could select the elements to which they committed. One concern is that any such commitments may deprive the source country of the regulatory flexibility needed in an area where both technology and concerns are evolving. A suitable balance between predictability and flexibility can be struck in at least two ways. The first is to allow regulatory commitments to be modified after a certain period or when there is a demonstrable need. The second is to state the regulatory commitments in the form of principles – as e.g. articulated in the OECD and APEC privacy principles – rather than as precise requirements.

iii. *Data source country recognition of conformity assessment in data destination countries*: In this case, the data source country unilaterally specifies privacy protection conditions but recognizes the procedures of the destination to assess conformity with those standards. This scenario can arise when there is divergence of norms between countries but trust in enforcement. The Safe Harbor/Privacy Shield agreement is an example because the EU accepted the US ability to ensure compliance with EU standards even though the US *national* privacy regulation was not deemed adequate. Such selective, country-specific recognition agreements are permitted under GATS Art. VII, but the provision requires that the data source country not use them to discriminate against other jurisdictions where similar conditions prevail and grant other countries the opportunity also to accede such agreements.

iv. *Collective additional commitments based on a convergence of regulatory requirements*: If there is sufficient similarity in privacy standards between a set of countries, they could develop a set of common requirements while each retains the right to unilaterally determine conformity by data destination countries. The OECD privacy principles are an example of a convergence in requirements, and the Telecommunications Reference Paper took the form of a collective legal commitment by a significant share of the WTO membership.

In fact, progress towards common privacy principles in APEC, OECD and the EU could form the basis of a WTO Reference Paper on Privacy. However, there is an important difference with the telecommunications precedent. The WTO Telecom Reference paper sought to ensure that the regulatory framework in importing countries, e.g. relating to interconnection between telecom networks, did not undermine their market access commitments. By committing to a Privacy Reference Paper, data source countries would specify the regulatory conditions that data destination countries would need to fulfil in order to be eligible for data transfers.

v. *Convergence of requirements and recognition of conformity assessment*: This situation combines the previous two options. The APEC approach not just to privacy but also to other areas like labor mobility is an example, where principles are agreed collectively and countries recognize adherence by specific firms or sources countries. Other examples are to be found in the goods contexts, such as the authorized exporter program stipulated in the WTO Trade Facilitation Agreement Art. 7:7 and the relevant standards developed by the World Customs Organization.

vi. *Mutually binding obligations on source and destination countries a la the CPTPP*: The CPTPP reflects the bargain central to successful regulatory cooperation (as in the EU-US Privacy Shield): data destination countries would assume legal obligations to protect the privacy of foreign citizens in return for obligations on source countries not to restrict the flow of data. However, achieving this outcome may only be possible initially among small groups of countries and by small steps.

> Interestingly, the CPTPP commitment to non-discriminatory privacy protection extends to all users of electronic commerce (it is not limited only to users from TPP parties) and thereby provides a key element for extending the approach also to non-member countries. However, for the CPTPP to be most effective – which includes minimizing the need to rely on the exceptions provision – there must also be convergence between the privacy requirements of data-source countries and the standards to which data-destination countries are willing to subscribe. The CPTPP implicitly relies on and reinforces other international efforts, such as in APEC and the OECD, to reach agreement on common standards or principles of privacy protection. The so-called "referential," which identifies similarities and differences between the APEC CBPR and the use of BCRs under the EU Data Directive, is a complimentary way of developing interoperability amongst different privacy regimes (APEC 2014).

We would expect countries to self-select into these arrangements, as they are already doing in APEC, the OECD and Privacy Shield, and gradually widen and deepen them. In the transitional phase, multilateral rules would need to fulfil two important roles. GATS Articles III on transparency and VII on recognition agreements can help ensure that the emerging arrangements between sets of countries are fully transparent. More importantly, GATS Article VII can help ensure that any such arrangements do not discriminate against and are open to participation by third countries. The moment a country concludes an arrangement with one or more countries, as the EU has done vis-à-vis the US, it establishes a standard of treatment also vis-à-vis third countries. GATS Article VII's potential in this respect needs to be more widely recognized and more fully exploited by countries that are initially excluded from arrangements like the EU-US Privacy Shield.

VII. CONCLUSION

This paper has examined the implications of the European Union's new General Data Protection Regulation, with wider scope and stronger enforcement than in the earlier Data Protection Directive. By making international data transfers more difficult, strengthened regulation threatens developing countries' dynamic exports of services, particularly digitally delivered data processing and data-related business services. A more cooperative approach than the unilateral Data Directive and GDPR could help reconcile the EU's goal of privacy protection with the interests of its trading partners.

The GDPR confronts developing countries with a dilemma. If they seek an adequacy certification, then they must enact a national privacy law essentially equivalent to that of the EU, which Argentina, Uruguay and a few other countries have chosen to do. However, a national law imposes the same standard on all firms in the country, regardless of where they sell, at home or abroad. That could have adverse effects. The standard that is appropriate in an advanced country with well-developed markets and comprehensive access to services is not necessarily appropriate for a poor country. Prematurely stringent privacy laws could hurt the efficiency and development of financial and other markets by inhibiting the flow of information. Enacting such national privacy legislation would increase the economy-wide cost of doing business, which would hurt access to services at home and competitiveness in foreign markets which do not have EU-like privacy regulation. The experience of the Philippines discussed above reveals the difficulty in dealing with this dilemma.

If a country's national law fails the EU adequacy test, their firms will be required to use either Binding Corporate Rules (BCRs), designed for multinational companies to move data globally, or Standard

Contractual Clauses (SCCs) for each business deal. Both instruments require the levels of protection, oversight and access for individuals that would be offered in the EU. Both also require a data controller or processor, who can be held liable for breach, to be established in an EU Member State. And both routes are costly and time-consuming. The requirement of a presence in the EU increases costs and limits the benefits of seamless cross-border digital trade, especially for smaller firms. As the survey of Indian firms revealed, the result could be a significant loss of business opportunities.

How can the EU's legitimate need to protect privacy be fulfilled without obliging other countries to accept nation-wide EU standards or to incur the substantial compliance costs associated with SCCs and BCRs? Simply seeking commitments from governments to the free flow of data in trade agreements, is not a solution because data-source countries will not accept one-sided limits on their right to protect privacy. Traditional regulatory cooperation through harmonization and mutual recognition is not only unlikely but insufficient. As even identical regulations across countries do not by themselves address the problem that regulators cannot control the behavior of data-handling entities located outside their jurisdictions, and that regulators in these other jurisdictions are not mandated to look out for the interests of foreign citizens.

Instead of these traditional approaches, it may be more fruitful to build on a recent model of international cooperation. When the EU first enacted its privacy rules, privacy protection in the US was deemed inadequate and transatlantic data flows were threatened. In response, the EU and the US negotiated a Safe Harbor Agreement which was updated after the Snowden revelations as the Privacy Shield Agreement. At the heart of this deal is a promise by US firms to protect the privacy of European citizens to European standards in return for unrestricted data flows. The firms' commitment is monitored and enforced by US institutions, notably the Federal Trade Commission and the Department of Commerce.

Since the EU has recognized US conformity assessment mechanisms under the Privacy Shield, it has created a valuable opening. WTO law on services trade requires the EU to offer other countries an opportunity to negotiate comparable arrangements. Developing countries must take advantage of the opportunity, while strengthening their case for recognition by building the institutional capacity to credibly assess conformity.

A recognition agreement with the EU would have big advantages over existing options. First, unlike in the case of BCRS and SSCs, firms would not be required to establish a costly presence in the EU because the assessment of conformity with EU standards would take place at home by domestic regulators. Second, unlike in the case of national adequacy, firms would not be obliged to adopt more stringent and more costly standards for data involving transactions at home or with countries less demanding than the EU. Thus, countries would be free to tailor domestic standards to domestic needs and export standards to foreign needs.

In general, we would expect countries to proceed step-by-step in small groups, self-selecting into specific arrangements and gradually deepening them. As a first step, data source countries may continue to specify conditions unilaterally and determine conformity unilaterally, but lend additional transparency and predictability to their requirements by listing them, e.g. as Additional Commitments under Article XVIII of the GATS. A further step could be for data source countries to recognize conformity assessment in specific data destination countries when there is trust in enforcement even though norms diverge. In parallel, groups of countries, could also make collective additional commitments when they converge on regulatory requirements – say, in a WTO Reference Paper on

Privacy – building on OECD and APEC principles. These steps could pave the way ultimately for mutually binding obligations on source and destination countries as in the CPTPP.

Apart from any bilateral or plurilateral approach, there may also be scope for multilateral discussions, for example under the recent initiative on electronic commerce. Such discussions may help to gradually forge a broader consensus on both standards and mechanisms to ensure compliance.

VII. Bibliography

APEC (Asia Pacific Economic Cooperation). 2014. Joint work between experts from the Article 29 Working Party and from APEC Economies, on a referential for requirements for Binding Corporate Rules. https://www.apec.org/~/media/Files/Groups/ECSG/20140307_Referential-BCR-CBPR-reqs.pdf

APEC (Asia Pacific Economic Cooperation). 2017. "Privacy Framework." file:///C:/Users/CConstantine/Downloads/05_ecsg_privacyframewk.pdf

Appellate Body Report, Brazil-Measures Affecting Imports of Retreaded Tyres, WT/DS332/AB/R, adopted 17 December 2007.

Basu, Nayanima. 2013. "Data Adequacy Grant to India Non-Negotiable, Says EU envoy." The Business Standard. 17 May. http://www.business-standard.com/article/economy-policy/data-adequacy-grant-to-india-non-negotiable-says-eu-envoy-113051700013_1.html

Bauer, Matthias, Fredrik Erixon, Michal Krol, Hosuk Lee-Makiyama, and Bert Verschelde. 2013. "The Economic Importance of Getting Data Protection Right: Protecting Privacy, Transmitting Data, Moving Commerce." European Center for International Political Economy. https://www.uschamber.com/sites/default/files/documents/files/020508_EconomicImportance_Final_Revised_lr.pdf

Bauer, Matthias, Hosuk Lee-Makiyama, Erik van der Marel and Bert Verschelde. 2014. "The costs of Data Localisation: Friendly Fire on Economic Recovery, ECIPE Occasional Paper No. 3/2014

Bennet, Steven C. 2012. The Right to Be Forgotten: Reconciling EU and US Perspectives." Berkeley Journal of International Law. Vol 30, No. 1. http://scholarship.law.berkeley.edu/bjil/vol30/iss1/4

Castro, Daniel and Alan McQuinn. 2015. "Cross-Border Data Flows Enable Growth in All Industries." The Information Technology & Innovation Foundation (ITIF). http://www2.itif.org/2015-cross-border-data-flows.pdf.

Castro, Daniel. 2013. "The False Promise of Data Nationalism." Information Technology & Innovation Foundation (ITIF). http://www2.itif.org/2013-false-promise-data-nationalism.pdf.\

CBPRs (Cross Border Privacy Rules System). 2015. "For Business." http://www.cbprs.org/Business/BusinessDetails.aspx

Cory, Nigel. 2017. *Cross-Border Data Flows: Where Are the Barriers, and What Do They Cost?*" http://www2.itif.org/2017-cross-border-data-flows.pdf citing ECIPE 2014. Distribution Services for Certain Publications and Audiovisual Entertainment Products. https://www.wto.org/english/tratop_e/dispu_e/363abr_e.doc

EC (European Commission). 2001. Commission Decision on the adequate protection of personal data provided by the Canadian Personal Information Protection and Electronic Documents Act. Official Journal of the European Communities. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32002D0002&from=en

EC (European Commission). 2003. Implementing Decision of the European Parliament and of the Council on the adequate protection of personal data in Argentina. Official Journal of the European Communities. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32003D0490

EC (European Commission). 2011. Implementing Decision of the European Parliament and of the Council on the adequate protection of personal data by the State of Israel with regard to automated processing of personal data. Official Journal of the European Communities. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32011D0061&from=EN

EC (European Commission). 2012. Implementing Decision of the European Parliament and of the Council the European Parliament and of the Council on the adequate protection of personal data by New Zealand. Official Journal of the European Communities. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32013D0065&from=EN

EC (European Commission). 2012. Implementing Decision of the European Parliament and of the Council on the adequate protection of personal data by the Eastern Republic of Uruguay with regard to automated processing of personal data. Official Journal of the European Communities. http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2012:227:0011:0014:EN:PDF

EC (European Commission). 2012. Proposal for a Regulation of the European Parliament and of the Council on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data. http://eur-lex.europa.eu/legal-content/HR/ALL/?uri=celex:52012PC0011

EC (European Commission). 2012. Commission Implementing Decision of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield. Official Journal of the European Communities. https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016D1250&from=EN

EC (European Commission). 2017. EU – U.S. Privacy Shield – First annual Joint Review. Article 29 Data Protection Working Party, WP255. https://ec.europa.eu/newsroom/just/document.cfm?doc_id=48782

EC (European Commission). 2017a. Communication from the Commission to the European Parliament and the Council. Exchanging and Protecting Personal Data in a Globalised World. COM(2017) 7 final

.

OECD (2014), Measuring the Digital Economy: A New Perspective, OECD Publishing

Eichengreen, Barry and Poonam Gupta. 2010. “The Service Sector as India’s Road to Economic Growth?” India Council for Research on International Economic Relations, Paper No. 249. http://www.nber.org/papers/w16757

EU (European Union). 2018. GDPR Portal. https://www.eugdpr.org/

EU (European Union). 2018. General Data Protection Regulation. https://gdpr-info.eu/

European High Court. 2016. Between the Data Protection Commissioner and Facebook Ireland Limited and Maximillian Schrems. No. 4809. http://www.europe-v-facebook.org/sh2/HCJ.pdf

European Parliament and Council. 1995. Directive 95/46 on the protection of individuals with regard to the processing of personal data and on the free movement of such data. Official Journal of the European Communities. http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:31995L0046&from=en

European Union Court of Justice. 2014. *Google Inc v. Agencia Espanola de Proteccion de Datos*, C131/12 (2014).

European Union Court of Justice. 2015. Press Release No. 117/15, Luxembourg, 6 October 2015, Judgement in Case C-362/14, *Maximillian Schrems v Data Protection Commissioner*.

Greenleaf, Graham, D Korff, and I Brown. 2010. “Different Approaches to New Privacy Challenges in Particular in the Light of Technological Developments – Country Studies B.4 India.” European Commission D-G Justice, Freedom and Security.

Greenleaf. Graham. 2012. “The Influence of European Data Privacy Standards Outside Europe: Implications for Globalization of Convention 108.” University of Edinburgh School of Law Research Paper Vol. 2, No. 2. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1960299

Justice K S Puttaswamy v. Union of India and Ors, Supreme Court of India, Writ Petition (Civil) No. 494. http://supremecourtofindia.nic.in/pdf/LU/ALL%20WP(C)%20No.494%20of%202012%20Right%20to%20Privacy.pdf

Kshetri, Nir. 2010. "Cloud Computing in Developing Economies.” IEEE Computer, October 43(10), pp. 47-55. https://libres.uncg.edu/ir/uncg/f/N_Kshetri_Cloud_2010.pdf

Mattoo, Aaditya, and Sacha Wunsch. 2004. “Pre-empting Protectionism in Services: The WTO and Outsourcing.” Policy Research Paper 3237.

NASSCOM-DSCI (National Association of Software and Services Companies - Data Security Council of India). 2013. Survey of the Impact of EU Privacy Regulation on India’s Services Exporters.

OECD (Organization for Economic Cooperation and Development). 2013. *Data Driven Innovation: Big Data for Growth and Well-Being*. Paris: OECD Publishing.

OECD (Organization for Economic Cooperation and Development). 2013. *Recommendations of the Council Concerning Guidelines Governing the Protection of Privacy and Trans-border Flows of Personal Data*. https://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf

OECD (Organization for Economic Cooperation and Development). 2013. *The Evolving Privacy Landscape: 30 Years After the OECD Privacy Guidelines*, in The OECD Privacy Framework. https://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf

Privacy Shield Framework. 2018. "Privacy Shield Overview." https://www.privacyshield.gov/Program-Overview

Reserve Bank of India. 2017. "Survey on Computer Software & Information Technology Enabled Services Exports: 2016-17." https://www.rbi.org.in/scripts/BS_PressReleaseDisplay.aspx?prid=42513

Reserve Bank of India. 2016. *Withdrawal of Legal Tender Status for 500 and 1000 Notes: RBI Notice*. -https://rbi.org.in/Scripts/BS_PressReleaseDisplay.aspx?prid=38520.

Robert Howse. 2002. "The Appellate Body Rulings in the Shrimp/Turtle Case: A New Legal Baseline for the Trade and Environment Debate." Columbia Journal of Environmental Law. Vol 27: 2.

Schrems v. Data Protection Commissioner, Court of Justice of the European Union, C362/14, 6 (2015).

Schwartz, Paul M. 2013. "Information Privacy in the Cloud." *University of Pennsylvania Law Review,* Vol. 161, No. 6. http://scholarship.law.upenn.edu/penn_law_review/vol161/iss6/5

U.S. Department of Commerce. 2016. E.U.-U.S. Privacy Shield Framework Principles, Issued by the U.S. Department of Commerce. https://www.privacyshield.gov/servlet/servlet.FileDownload?file=015t00000004qAg

USFTC (U.S. Federal Trade Commission). 2015. "Internet of things, Privacy and Security in a Connected World." https://www.ftc.gov/system/files/documents/reports/federal-trade-commission-staff-report-november-2013-workshop-entitled-internet-things-privacy/150127iotrpt.pdf

USITC (U.S. International Trade Commission). 2014. Digital Trade in the U.S. and Global Economies, Part 2. https://www.usitc.gov/publications/332/pub4485.pdf

Warren, Samuel D. Warren and Louis D. Brandeis. 1890. "The Right to Privacy." *Harvard Law Review,* -Vol. 4, No. 6. https://www.english.illinois.edu/-people-/faculty/debaron/582/582%20readings/right%20to%20privacy.pdf

World Economic Forum. 2014. "Rethinking Personal Data: A New Lens for Strengthening Trust." In collaboration with A.T. Kearney. -http://www3.weforum.org/docs/WEF_RethinkingPersonalData_ANewLens_Report_2014.pdf.

WTO (World Trade Organization). 1995. Understanding on commitments in financial services. https://www.wto.org/english/tratop_e/serv_e/21-fin_e.htm

WTO (World Trade Organization). 2001. United States — Import Prohibition of Certain Shrimp and Shrimp Products. https://www.wto.org/english/tratop_e/dispu_e/cases_e/ds58_e.htm

WTO (World Trade Organization). 2007. Brazil – Measures Affecting Imports of Retreaded Tyres. https://www.wto.org/english/tratop_e/dispu_e/332abr_e.doc

WTO (World Trade Organization). 2012. China – Measures Affecting Trading Rights And Distribution Services for Certain Publications and Audiovisual Entertainment Products. https://www.wto.org/english/tratop_e/dispu_e/363abr_e.pdf

WTO (World Trade Organization). 2014. European Communities - Measures Prohibiting the Importation and Marketing -of Seal Products. https://www.wto.org/english/tratop_e/dispu_e/400_401abr_e.pdf

WTO (World Trade Organization). 2009. Panel report in United States-Gambling; WTO Appellate Body decision in China-Audiovisuals. https://www.wto.org/english/tratop_e/dispu_e/363abr_e.pdf

WTO (World Trade Organization). 1995. General Agreement on Trade in Services. -https://www.wto.org/english/res_e/booksp_e/analytic_index_e/gats_02_e.htm#article14