University of Miami International and Comparative Law Review

Volume 28
Issue 1 *Fall 2020*

Article 6

2-17-2021

Privacy Before Trade: Assessing the WTO-Consistency of Privacy-Based Cross-Border Data Flow Restrictions

Julian Rotenberg

PRIVACY BEFORE TRADE: ASSESSING THE WTO-CONSISTENCY OF PRIVACY-BASED CROSS-BORDER DATA FLOW RESTRICTIONS

Julian Rotenberg[*]

ABSTRACT

The first decades of the 21st century have been characterized by the growth of digital trade fueled by new business models based on cross-border data flows. With data taking a central role in the digital economy, governments and their constituents have become increasingly concerned about the commercial handling and commoditization of personal data. Consequently, governments have entered the business of regulating cross-border data flows, especially with the aim of protecting the privacy of their citizens. This regulatory trend does not occur in a vacuum: The World Trade Organization (WTO) through the General Agreement on Trade in Services (GATS) regulates the types of measures and treatment that governments may adopt regarding foreign providers of digital services. Further, several Free Trade Agreements (FTAs) include electronic commerce or digital trade chapters establishing obligations regarding cross-border data flows. This paper focuses on cross-border data flow restrictions aimed at protecting privacy and the assessment of their WTO-consistency. This perspective covers a broader range of measures and offers a more comprehensive understanding of privacy regulations before trade fora than the existing literature does. In particular, this paper draws attention to the assessment of privacy-based restrictions under the GATS exceptions and argues that the necessity test and chapeau requirements will prove critical in any future adjudication over complaints against a country's policies restricting cross-border data transfers. This analysis highlights that the linkage between trade and privacy will continue to intensify and that this linkage will be further shaped by countries being taken to court.

---

[*] Foreign Associate, Freshfields Bruckhaus Deringer (Washington, DC). Lawyer (University of Buenos Aires), LL.M. (Harvard Law School). The article represents only the author's views and not necessarily the views of the firm or any of its clients.

I. INTRODUCTION

The first decades of the 21st century have been characterized by the growth of digital trade fueled by, and in turn contributing to the expansion of, new business models based on cross-border data flows. With data taking a central role in today's digital economy, governments and their constituents have become increasingly concerned about the commercial handling and commoditization of personal data. Consequently, governments around the world have entered the business of regulating cross-border data flows, especially with the aim of protecting the privacy of their citizens.

This regulatory trend does not occur in a vacuum. Most countries in the global economy are members of the World Trade Organization (WTO), which under the General Agreement on Trade in

Services (GATS) regulates the types of measures and treatment that countries can adopt regarding foreign providers of digital services. Further, several countries are parties to Free Trade Agreements (FTAs) that include electronic commerce or digital trade chapters establishing obligations regarding cross-border data flows.

Data flows and data protection are central components of economic and trade policy in the digital era. When a country restricts cross-border data transfers with the aim of protecting privacy, it might incur breaches of legal obligations owed to other countries and firms. Considering the relevance of cross-border data flows and the potential economic impact of restrictions, countries may soon begin to face international litigation against their measures. On an inter-state basis, this could occur at the multilateral level before the WTO Dispute Settlement Body. It could also occur at the regional or bilateral level, under an FTA replicating the GATS framework or otherwise governing data regulations. Although beyond the scope of this paper, these measures might also give rise to litigation by foreign firms under International Investment Agreements (IIAs) providing for investor-state arbitration.

Until recently, scholarly studies of international trade law and privacy have remained independent from each other. An emerging literature is now beginning to trace the connections between these two fields, focusing on the applicability of the GATS framework to privacy and cybersecurity laws.[1] However, most of these efforts have tended to focus on data localization measures, while other types of privacy-based restrictions have not been sufficiently addressed.

This paper contributes to bridging this gap by focusing on cross-border data flow restrictions aimed at protecting privacy and the

---

[1] *See, e.g.,* Neha Mishra, *Privacy, Cybersecurity, and GATS Article XIV: A New Frontier for Trade and Internet Regulation?*, WORLD TRADE REVIEW 1 (2019); Ines Willemyns, *The GATS (In)Consistency of Barriers to Digital Services Trade*, 207 LEUVEN CTR. FOR GLOBAL GOVERNANCE STUDIES WORKING PAPER (2018), https://ghum.kuleuven.be/ggs/publications/working_papers/2018/wp207-willemyns.pdf; Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, INT'L CTR. FOR TRADE AND SUSTAINABLE DEV. & WORLD ECON. F. E15INITIATIVE (2016), http://e15initiative.org/wp-content/uploads/2015/09/E15-Policy-Brief-Crosby-Final.pdf; Diane A. MacDonald, & Christine M. Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUSTON J. INT'L L. 625 (2014).

assessment of their WTO-consistency. This perspective covers a broader range of measures than data localization requirements and offers a more comprehensive understanding of privacy regulations before trade fora than the existing literature does.

The paper draws attention to the need to assess privacy-based restrictions under the GATS exceptions. It argues that the necessity test and the chapeau requirements will prove critical in any future adjudication over complaints against a country's policies restricting cross-border data transfers, emphasizing the need for countries to focus on this line of argumentation. This analysis highlights that the linkage between trade and privacy will continue to intensify and that this linkage will be further shaped by countries being taken to court.

Part II provides an introduction to cross-border data flows regulation and the taxonomies by which to classify them. Part III addresses cross-border data flows regulation aimed at protecting privacy, analyzing the regulatory approaches of adequacy and accountability. Part IV discusses the framing of these measures under the WTO services regime, surveying the main applicable provisions of the GATS and then focusing on possible claims regarding WTO-inconsistency, ultimately arguing that the necessity test and the chapeau requirements in the GATS exceptions will prove the highest hurdle for a respondent country.

II. CROSS-BORDER DATA FLOWS REGULATION

This Part introduces the concept of cross-border data flows regulation in the context of international trade. It also reviews some of the taxonomies that have been proposed to classify regulatory approaches around the globe, setting the scene for the analysis of privacy-based restrictions in the next Part.

Cross-border data flow regulations are employed by governments around the world in response to a variety of concerns such as cybersecurity, privacy, banking and financial supervision, consumer protection, or economic protectionism, to name a few.[2]

[2] *See, e.g.*, Anupam Chander & Uyen P. Le, *Data Nationalism*, 64(3) EMORY L. J. 677, 713 (2015).

Although privacy-based restrictions on data transfers[3] have generally been analyzed from the perspective of data protection law, addressing them as a subset of cross-border data flow regulations places these restrictions within a broader regulatory context and helps assess them in the light of the trade regime.

The OECD defines cross-border data flow regulations as "measures that affect the possibility of exchanging and moving data across borders."[4] In terms of trade, restrictions on data flows have the effect of raising the cost of conducting business across borders by obligating companies to store data within a country's territory or imposing requirements for data to be transferred abroad.[5]

Several different taxonomies have been proposed to group the variety of regulatory approaches to cross-border data transfers adopted around the world. Despite differences in criteria, all classifications identify the extent of regulatory interference with data transfers as the key factor. Regulatory approaches are generally placed along a spectrum of increasing regulatory presence, ranging from a total absence of regulation, to moderate levels of regulatory incursion, and up to highly restrictive regimes. There is not one single taxonomy of cross-border data regulations that can be singled out as the most precise to the exclusion of all others; they are all useful models to analyze differing approaches. Since these taxonomies are drawn from real-world cases, they serve as frameworks to better understand how the varying degrees of government intervention affect data transfers.

The taxonomy set forth by the OECD focuses on the degree of restrictiveness. It is composed of three main categories: regulations allowing for the free flow of data; regulations making data flow conditional on safeguards; and regulations making data flow

---

[3] Although there are distinctions between personal data protection and privacy protection, for the purposes of this paper the two concepts are employed interchangeably.

[4] Francesca Casalini & Javier Lopez Gonzalez, TRADE AND CROSS-BORDER DATA FLOWS, OECD TRADE POLICY PAPERS, NO. 220, 11, OECD PUB. (2019), https://read.oecd-ilibrary.org/trade/trade-and-cross-border-data-flows_b2023a47-en#page11 [hereinafter OECD Report].

[5] Martina Ferracane, *Restrictions on Cross-Border data flows: a taxonomy* 2 (ECIPE, Working Paper No. 1, 2017), https://ecipe.org/wp-content/uploads/2017/11/Restrictions-on-cross-border-data-flows-a-taxonomy-final1.pdf.

conditional on *ad-hoc* authorization.[6] The types of regulations that may present trade law challenges will fall under the second and third categories, which present tangible government action and imposition of restrictions on cross-border transfers. The second category comprises approaches that require the fulfilment of certain conditions to allow for data transfers; there are different subcategories depending on the responsible authority and the method for establishing these conditions, and the alternative means available for transfers in the absence of such conditions. Generally, these subcategories include adequacy or equivalence findings by private entities or government agencies, and alternatives like undertakings by data exporters, contractual agreements, or data subject consent. The third category comprises approaches that limit the alternatives to an adequacy finding by a public authority, requiring *ad-hoc* government approval or directly subjecting all transfers to government review.

Another taxonomy, proposed by Martina Ferracane, focuses on the nature of the restrictions to cross-border data flows and classifies them into strict and conditional. Strict restrictions are those imposing data localization requirements or banning transfers outright, while a conditional regime subjects cross-border transfers to certain conditions.[7] The types of privacy-oriented regulations that are the focus of this paper will generally fall under the second group. These conditions might be applicable to the country where the data will be received, the company carrying out the transfers, or both the recipient country and the company. Data flows regimes usually require the fulfilment of one specific condition or one among alternative options, but in some cases the conditions might be so stringent as to result in an outright ban on the transfer.

Finally, Christopher Kuner distinguishes between two opposing "default regulatory positions" in cross-border data flow regulations. On one end are frameworks that allow data transfers by default and enable regulators to block or limit them, while on the other are those that prohibit data flows unless there is a specific legal basis for transfer.[8] Writing from the standpoint of privacy, Kuner proposes

---

[6] OECD Report, *supra* note 4, at 16-21.
[7] Ferracane, *supra* note 5, at 3-4.
[8] CHRISTOPHER KUNER, TRANSBORDER DATA FLOWS AND DATA PRIVACY LAW 76 (2013).

a classification of cross-border data flow regulations that aligns neatly with Ferracane's definition of conditional regimes with restrictions applicable either to the recipient country or to the entity handling the data. This classification will be the basis of the next Part.

III. PRIVACY-BASED DATA RESTRICTIONS

This Part deals with cross-border data flow regulations particularly addressing privacy. It first introduces the two main regulatory approaches to privacy-based restrictions, adequacy and accountability, and then surveys comparative examples of each model.

The most salient model to assess "privacy protection frameworks addressing cross-border data transfers"[9] has been proposed by Kuner, who distinguishes between "geographically-based" and "organizationally-based" approaches.[10] The geographically-based or "adequacy" approach focuses on the country or location where the data are transferred; it is the one adopted by the EU and several other countries. It presents a variety of tests applied to the legal regime of the receiving country turning on its adequacy, equivalence, or comparability to the home jurisdiction. The organizationally-based or "accountability" approach focuses on the entities and organization that control the data; it is most prominently featured in the APEC Privacy Framework, entrusting data exporting companies with guaranteeing a certain level of treatment on the personal data that is transferred. Several privacy regimes present an overlap or coexistence between both approaches by offering the choice between alternative mechanisms for data transfers. The GDPR, for instance, adopts an adequacy requirement but also recognizes accountability instruments like binding corporate rules and standard contractual clauses.

A. Geographically-Based or Adequacy Approach

The geographically-based approach regulates data transfers based on the level of data protection in place in the receiving or

---

[9] Rolf H. Weber, *Regulatory Autonomy and Privacy Standards under the GATS*, 7 ASIAN J. WTO & INT'L HEALTH L. & POL'Y 25, 31 (2012).
[10] KUNER, *supra* note 8, at 64-76.

importing country. According to this approach, the legal system of the receiving or importing country must assure a certain level of protection comparable to that of the exporting country for transfers to be permitted.[11]

This condition is met by establishing the adequacy or equivalence between the two legal frameworks. Although generally discussed jointly, equivalence entails a level of objective similarity between two regulations in terms of tools used and objectives of the regulation while adequacy is more flexible as it focuses on a common agreed outcome but allows for different tools to achieve it. The most famous example of this model is the requirement of an "adequate level of protection" established by the EU,[12] and hence this approach is generally identified as "adequacy."

The adequacy of the receiving country's level of data protection is usually determined by a public body such as the data protection authority or a higher political authority. Such determination can be adopted as a unilateral recognition, with one country establishing the adequacy of another and allowing the transfer of data to that destination, or a mutual recognition between two or more countries enabling free flows of data among them. This mutual type of recognition can be implemented through an arrangement between data protection agencies or be included in a broader agreement such as an FTA.

In practical terms, the adequacy approach implies that the domestic data protection laws of one country or jurisdiction will determine the minimum standards that others must meet in order to be recipients of data transfers from it. Thus, this approach could be used by a government as an incentive for others to enact data protection laws with a certain content in order to attract data exports. When the sovereign enacting the baseline level of protection has a significant trade and political influence, this approach serves as an effective way of exporting its regulatory standards. In fact, encouraging the adoption of similar regulation by other countries is cited as motivating the inclusion of this approach in the earlier EU Directive.[13]

---

[11] *Id.*

[12] *Id.*; *see infra* Part III.C.i.

[13] KUNER, *supra* note 8, at 66.

When considering the economic and business implications of an adequacy determination, it is easy to see the potential political underpinnings of any such decision. A country's determination of whether another country provides a comparable, equivalent, or adequate level of protection to personal data is a kind of judgment on a foreign regulatory system which may well be guided by political considerations. In the EU context, Kuner documents some examples of politics influencing adequacy determinations by the Commission.[14]

Therefore, the procedures by which adequacy or equivalence decisions are adopted play an important role, especially when measured by objective standards as mandated by WTO caselaw. For instance, the OECD states that very few countries establish publicly the substantive criteria used to determine adequacy in data protection laws and regulations and recommends that these criteria and processes should be transparent, non-discriminatory, and avoid unnecessary trade restrictiveness, among other conditions.[15]

The adequacy approach does not generally appear as the sole mechanism for data transfers within individual privacy regimes. Countries that follow this approach tend to also offer alternative accountability mechanisms to enable data transfers in the absence of an adequacy determination, such as contractual arrangements or the consent of the data subject.

B. Organizationally Based or Accountability Approach

The organizationally based approach regulates the treatment by companies and other organizations of the data that is transferred across borders. These organizations are made "accountable" for the processing of personal data according to specified privacy principles regardless of the location where the data are processed.[16] The accountability approach does not restrict cross-border data flows but imposes responsibilities on the parties that transfer data.

Under this approach, the protection is based on specific obligations established under the law of the data controller that continue to apply to the personal data after it crosses national borders.

---

[14] *Id*.
[15] OECD Report, *supra* note 4, at 20.
[16] KUNER, *supra* note 8, at 71.

The specific principles vary among different models following this approach, as do the ways of instrumenting these obligations. Two common forms of the accountability approach are binding corporate rules and standard contractual clauses.

Binding corporate rules impose obligations on companies with operations in different countries in terms of data protection. Adopting and implementing binding corporate rules allows multinational firms to move data across borders - although only among the firms' affiliates in different countries - independently of the individual countries' consideration of one another's data protection frameworks. These instruments usually must be previously approved by data protection authorities in the countries involved, which can involve lengthy procedures.[17]

Standard contractual clauses are rules used in transactions involving the cross-border transfer of personal data to third parties. These clauses are usually developed or approved by data protection authorities and, upon their inclusion in contracts, are deemed as sufficiently protective of the data that are transferred, regardless of the destination country. They are a convenient mechanism in terms of applicability but may include onerous conditions and increase administrative costs.[18]

Accountability instruments are often established in privacy regimes as safeguards or alternative mechanisms to enable cross-border data transfers in the absence of another "main" legal ground such as an adequacy finding.

C. Comparative Examples[19]

i. Adequacy: The European Union

The regime that gives name to the adequacy approach is the EU, currently governed by the General Data Protection Regulation

[17] OECD Report, *supra* note 4, at 21.
[18] *Id.* at 22.
[19] *See generally* Ferracane, *supra* note 5, at 10-27; Rachel F. Fefer, *Data Flows, Online Privacy, and Trade Policy*, R45584 CONGRESSIONAL RESEARCH SERVICE (Mar. 26, 2020), https://crsreports.congress.gov/product/pdf/R/R45584; GLOBAL LEGAL GROUP, THE INTERNATIONAL COMPARATIVE LEGAL GUIDE TO: DATA PROTECTION

(GDPR).[20] Under the GDPR, personal data can be transferred from the EU to third countries that provide an "adequate level of protection,"[21] which must be established through an adequacy finding by the European Commission. The considerations that go into an adequacy finding are also listed in the GDPR and include the existence of the rule of law; legislation including public security, national security, and 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.[22]

While adequacy determinations may take into account different approaches to privacy protection such as self-regulation by firms, in practice such findings have all been made regarding countries whose privacy regimes are essentially equivalent to the EU:[23] comprehensive laws that provide a level of data protection, government access and rights of redress consistent with EU standards.

An adequacy finding may also be made with respect to specific economic sectors or territories within a third country,[24] which until recently covered the EU-US Privacy Shield. Concluded in 2016, the EU-US Privacy Shield governed transfers of personal data between the EU and participating businesses in the United States.[25] Though not a third country national framework, the Privacy Shield *per se* was originally found by the European Commission as providing an adequate level of

---

2019 (6th ed. 2019); Aaditya Mattoo & Joshua P. Meltzer, *International Data Flows and Privacy. The Conflict and Its Resolution*, WORLD BANK GROUP POLICY RESEARCH WORKING PAPER 8431, 25-26 (2018), http://documents.worldbank.org/curated/en/751621525705087132/pdf/WPS8431.pdf.

[20] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation), 2016 O.J. (L 119) 1, https://eur-lex.europa.eu/eli/reg/2016/679/oj [hereinafter GDPR].

[21] *Id.* at Article 45.

[22] *Id.* at Article 45.2.

[23] Mattoo & Meltzer, *supra* note 19, at 9.

[24] GDPR, *supra* note 20, at Article 45.3.

[25] The Privacy Shield was adopted to replace the EU-US Safe Harbor arrangement after it was found by the Court of Justice of the EU as not providing an adequate level of protection. *See* Court of Justice of the European Union Case C-362/14, Maximilian Schrems v. Data Prot. Comm'r, ECLI:EU:C:2015:650, http://curia.europa.eu/juris/liste.jsf?num=C-362/14.

protection, but was recently invalidated by the Court of Justice of the EU.[26] This arrangement established a series of principles, largely reflecting EU law, with which U.S. companies self-certified to the U.S. Department of Commerce that they would comply in processing personal data.[27] These features make such an arrangement more challenging to classify, as the data transfers are allowed by an adequacy finding but the actual obligations and responsibilities are undertaken by the businesses, which could suggest listing this approach as an organizationally-based one.

The GDPR also provides a series of safeguards to enable cross-border transfers to countries that do not have an adequacy finding:[28] binding corporate rules, contractual clauses, codes of conduct, and certification mechanisms. These are accountability instruments that seek to ensure protection based on EU law and that must be previously approved by the Commission or a Member State's privacy authority.

Binding corporate rules (BCRs) are policies consistent with the GDPR 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.[29] BCRs must be legally applied and confer enforceable rights on data subjects,[30] and there must exist a controller or processor established in a Member State who can be held liable for breach.[31]

While BCRs are only available for transfers among corporate affiliates, standard contractual clauses (SCCs) are available to all companies, and they should ensure the same levels of protection,

---

[26] Commission Implementing Decision (EU) 2016/1250 of 12 July 2016 pursuant to Directive 95/46/EC of the European Parliament and of the Council on the adequacy of the protection provided by the EU-U.S. Privacy Shield, 2016 O.J. (L 207) 1; *see* Court of Justice of the European Union Case C-311/18, Data Prot. Comm'r v. Facebook Ireland Ltd., Maximilian Schrems, ECLI:EU:C:2020:559, ¶¶ 1-16 (July 16, 2020).

[27] *Id*. at ¶¶14-63.

[28] GDPR, *supra* note 20, at Article 46.

[29] *Id.* at Article 47.

[30] *Id.* at Article 47.2.

[31] *Id.* at Article 47.2(f).

oversight and access for individuals consistent with the GDPR as an adequacy decision would.[32]

Codes of conduct can apply to associations representing controllers or processors and can be used to ensure compliance with the GDPR standards.[33] These instruments must be approved by the Commission and be subject to monitoring and enforcement by an accredited entity within a Member State.[34]

Certification mechanisms allow the development of data protection seals and marks to demonstrate compliance with GDPR by processors and controllers within the EU. These mechanisms can also be used by businesses outside of the EU and serve as a basis for data transfers.[35]

Finally, the GDPR also contains exceptions ("derogations") to circumvent these requirements, including consent by the data subject and transfers necessary to perform a contract or for the purpose of a legitimate interest, among others.[36]

ii. Other Adequacy Models

There are several other examples of the adequacy approach following the EU model, with variations and sometimes similar safeguards or alternatives.

In Switzerland, personal data may only be transferred to countries that provide an "adequate" level of protection, or pursuant to other arrangements such as a contract or binding corporate rules, for specific public policy purposes, or with the data subject's consent.[37] Russia's Data Protection Law, besides establishing local storage and processing requirements,[38] allows transfers to countries that Russia

[32] *Id.* at Article 46.2(c)-(d).
[33] GDPR, *supra* note 20, at Article 40.
[34] *Id.* at Article 41.
[35] *Id.* at Article 42.
[36] *Id.* at Article 49.
[37] BUNDESGESETZ ÜBER DEN DATENSCHUTZ [DSG], LOI FÉDÉRALE SUR LA PROTECTION DES DONNÉES [LPD], LEGGE FEDERALE SULLA PROTEZIONE DEI DATI [LPD] [FEDERAL ACT ON DATA PROTECTION (FADP)] Jun. 19, 1992, SR 235.1, Art. 6 (Switz.).
[38] Federal'nyi Zakon RF ot 21 iiulia 2014 g. No. 242-FZ [Federal Law of the Russian Federation of 21 July 2014 No. 242-FZ], SOBRANIE ZAKONODATEL'STVA ROSSIISKOI

recognizes as offering adequate protection or that are parties to the Council of Europe Convention 108,[39] or with prior consent of the data subject. [40]

In Israel, transfers are permitted to EU Member States, other parties to Council of Europe Convention 108, and other countries that are recipients from EU Member States. Apart from these, transfers are permitted with data subject consent or as part of contractual arrangements ensuring compliance with Israeli standards.[41] In Turkey, personal data cannot be processed or transferred abroad without the individual's consent; but it is not required where the transfer is necessary to exercise a right or is required by law, and the recipient country provides sufficient protection or the data controller makes a security undertaking and is granted permission by Turkey's Personal Data Protection Board.[42]

Under Singapore's Personal Data Protection Act, a company may only transfer personal data to recipient countries that provide a "comparable" level of protection (or with consent of the individual) and must ensure compliance with the Act's obligations while controlling the data. [43] In Japan, the Act on the Protection of Personal Information (APPI) allows transfers to countries designated as having an "acceptable" level of protection, to a third party abroad that ensures the same level of protection as in Japan, for example through contractual arrangements, or with the data subject's consent.[44]

In Latin America, several countries have followed the EU model closely. For instance, Argentina's Data Protection Law prohibits

---

FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2014, No. 30, Item 4243, Art. 2.

[39] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, Jan. 28, 1981, E.T.S. No.108.

[40] Federal'nyi Zakon RF ot 27 iiulia 2006 g. No. 152-FZ [Federal Law of the Russian Federation of 27 July 2006 No. 152-FZ], SOBRANIE ZAKONODATEL'STVA ROSSIISKOI FEDERATSII [SZ RF] [Russian Federation Collection of Legislation] 2006, No. 31, Item 3451, Art. 12.

[41] Protection of Privacy Law, 5741 – 1981, 5 LSI 136 (5741-1980/81) (Isr.); Privacy Protection (Transfer of Data to Databases Abroad) Regulations, 5761-2001, KT 6113 p. 900 (Isr.).

[42] Law on the Protection of Personal Data, Law No. 6698 of 2016, Art. 9 (Turk.).

[43] Personal Data Protection Act, Act No. 26 of 2012, Art. 26 (Sing.).

[44] Kojin jōhō no hogo ni kansuru hōritsu [Act on the Protection of Personal Information (APPI)], Act No. 57 of 2003, arts. 23-24 (Japan).

transfers to countries that do not provide an "adequate" level of protection,[45] which can be circumvented by agreement between the data controller and the foreign processor ensuring compliance with the local standards of protection, or with the data subject's consent.[46] Colombia also restricts transfers to countries that do not offer "adequate" standards of protection, except with express authorization by the data subject, for specific types of data or in the context of international conventions.[47] In Peru, transfers of personal data can only be made if the destination country offers "adequate" protection equivalent to the Personal Data Protection Law or international standards, if the controller ensures compliance with such standards (for example, contractually), or with the data subject's consent.[48]

iii. Accountability: The APEC CBPR

One of the most relevant examples of the accountability approach is the Cross-Border Privacy Rules (CBPR) mechanism adopted to facilitate personal data transfers among Asia-Pacific Economic Cooperation (APEC) countries. The CBPRs require businesses to develop policies based on the APEC Privacy Framework,[49] a set of guiding principles based on the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. The businesses' policies and practices must be certified by APEC Accountability Agents as consistent with the CBPR requirements; APEC Accountability Agents together with national Privacy Enforcement Authorities are responsible for enforcing compliance.[50] Any APEC country can agree to this system unilaterally,

---

[45] Law No. 25,326, Oct. 4, 2000, B.O. 29,517, Art. 12 (Arg.).
[46] Decree No. 1558, Nov. 29, 2001, B.O. 29,787, Art. 12 (Arg.).
[47] L. 1581/12, octubre 17, 2012, DIARIO OFICIAL [D.O.] 48587, Art. 26 (Colom.).
[48] Law No. 29,733, Jul. 2, 2011, E.P. 445746, Art. 15 (Peru).
[49] Asia-Pacific Economic Cooperation [APEC], *APEC Privacy Framework*, APEC#217-CT-01.9 (2015), https://www.apec.org/-/media/APEC/Publications/2017/8/APEC-Privacy-Framework-(2015)/217_ECSG_2015-APEC-Privacy-Framework.pdf.
[50] Asia-Pacific Economic Cooperation [APEC], *APEC Cross-Border Privacy Rules System* (2019), http://cbprs.org/wp-content/uploads/2019/11/4.-CBPR-Policies-Rules-and-Guidelines-Revised-For-Posting-3-16-updated-1709-2019.pdf; Asia-Pacific Economic Cooperation [APEC], *APEC Cross-Border Privacy Rules System*

and businesses that are subject to the country's laws will be able to use it. To date, the participating economies are the United States, Mexico, Canada, Japan, South Korea, Australia, Chinese Taipei, and Singapore.[51]

iv. Other Accountability Models

In Australia, a company transferring personal data abroad must take steps to ensure that the recipient will comply with the Australian Privacy Principles (APPs). This requirement is excepted if the recipient is bound by similar legal and enforceable requirements or the data subject consents, however a company may be held liable for breaches of the APPs by the recipient.[52]

In Canada, under the Personal Information Protection and Electronic Documents Act (PIPEDA), a company transferring data abroad must grant a comparable level of protection while it is processed by a third party, preferably through contractual arrangements. Data subject consent is not required as the law does not distinguish between domestic and international transfers.[53]

In New Zealand, consent is not required for data transfers to third countries in compliance with the Information Privacy Principles, but substantive protections continue to apply to the personal and health information even when outside of the country.[54]

South Africa requires data subject consent for cross-border transfers, but this can be waived if the recipient is subject to laws, binding corporate rules or agreements providing an adequate level of protection, or the transfer is necessary as part of a contract between the

---

Program Requirements (2019), http://cbprs.org/wp-content/uploads/2019/11/5.-Cross-Border-Privacy-Rules-Program-Requirements-updated-17-09-2019.pdf; Asia-Pacific Economic Cooperation [APEC], *APEC Cooperation Arrangement for Cross-Border Privacy Enforcement* (2019), http://cbprs.org/wp-content/uploads/2019/11/1.-Cross-Border-Privacy-Enforcement-Arrangement-updated-17-09-2019.pdf.

[51] ABOUT CBPRS, http://cbprs.org/about-cbprs/ (last visited May 12, 2020).

[52] Federal Privacy Act 1988 (Sch 1 Pt 3) s. 8 (Austl.).

[53] Personal Information Protection and Electronic Documents Act, S.C. 2000, c. 5, div 1, s. 5, Schedule 1 (Can.).

[54] Privacy Act 1993, s. 114B (N.Z.).

data subject and the responsible party or to implement pre-contractual measures following the data subject's request.[55]

IV. PRIVACY-BASED DATA RESTRICTIONS IN THE WTO FRAMEWORK

This Part places privacy-based cross-border data flow regulations within the multilateral trade regime. Although there are suggestions that some operations involving digital services could be considered as trade in goods,[56] the prevailing view identifies the services regime as the appropriate framework governing cross-border data flow regulations.[57] After an introduction to the WTO regulation of trade in services, this Part presents the possible discussions on the WTO-consistency of a measure and then focuses on the exceptions framework, which will be the ultimate line of argumentation for the legality of any such regulation.

A. The WTO Trade in Services Framework

Under the WTO regime, the GATS[58] establishes two types of obligations on Members: general obligations and specific commitments. General obligations are owed with respect to all Members and all sectors, while specific commitments are undertaken by Members for the sectors and modes of supply that they expressly set out.[59]

---

[55] Protection of Personal Information Act 4 of 2013 § 72 (S. Afr.).

[56] Andrew D. Mitchell, & Jarrod Hepburn, *Don't Fence Me In: Reforming Trade and Investment Law to Better Facilitate Cross-Border Data Transfers*, 19 YALE J. L. & TECH. 182, 196-97 (2017); MacDonald & Streatfeild, *supra* note 1, at 633.

[57] Mattoo & Meltzer, *supra* note 19, at 16; Crosby, *supra* note 1, at 2; Willemyns, *supra* note 1, at 6-12; Andrew D. Mitchell & Neha Mishra, *Data at the Docks: Modernizing International Trade Law for the Digital Economy*, 20 VAND. J. ENT. & TECH. L. 1073, 1088-97 (2018).

[58] General Agreement on Trade in Services, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, 1869 U.N.T.S. 183 [hereinafter GATS].

[59] MITSUO MATSUSHITA, THOMAS J. SCHOENBAUM, PETROS C. MAVROIDIS & MICHAEL HAHN, THE WORLD TRADE ORGANIZATION: LAW PRACTICE, AND POLICY 557-59 (3rd ed. 2015).

Among the general obligations, the most-favored-nation (MFN) principle established in Article II provides that Members must "accord immediately and unconditionally to services and service suppliers of any other Member treatment no less favorable than that it accords to like services and service suppliers of any other country."[60] The MFN obligation prevents Members from granting preferable treatment to some Members to the detriment of others.

This principle is subject to limited exceptions. Most importantly, Article V enables Members to conclude agreements further liberalizing trade in services as long as the agreements have substantial sectoral coverage and substantially eliminate all discrimination among the parties.[61] This provision is sister to GATT Article XXIV and provides the legal basis for services chapters in FTAs.[62]

As for the specific commitments, the method for liberalizing trade in services is fundamentally different from the goods regime. Under the GATT, each Member adopts a Schedule of Concessions that limits the tariffs that they may impose on goods from other Members.[63] By contrast, the GATS, reflecting a greater reluctance by Members to open their services markets, adopts a "positive list" approach[64] where each Member undertakes commitments to liberalize trade in specific sectors in its territory.[65]

In its Schedule of Specific Commitments, each Member must specify the terms, limitations, conditions, and time frames that it applies to each covered sector.[66] Moreover, specific commitments are undertaken not only by sector but also by mode of supply. The four modes of supply covered by the GATS, identified by their order in the list, are (1) cross-border, from one Member's territory into another Member's territory; (2) consumption abroad, in one Member's

---

[60] GATS, *supra* note 58, at Article II(1).
[61] *Id.* at Article V(1).
[62] MATSUSHITA, ET AL., *supra* note 59, at 573-76.
[63] GATS, *supra* note 58, at Article II.
[64] MacDonald & Streatfeild, *supra* note 1, at 633.
[65] In more recent agreements on services, this method has been gradually replaced by a "negative list" approach where parties by default undertake to liberalize all trade in services and must include in their schedules those sectors and modes that they wish to exempt.
[66] GATS, *supra* note 58, at Article XX.

territory to a consumer of another Member; (3) commercial presence, by one Member's service provider through the commercial presence in another Member's territory; and (4) presence of natural persons, by one Member's service supplier through the presence of natural persons in the territory of another Member.[67] Thus, within each possible sector, Members must also detail their commitments for each mode of supply of that service.

The main specific commitments are market access and national treatment.[68] Regarding market access in the specified sectors and modes, Article XVI requires each Member to "accord services and service suppliers of any other Member treatment no less favorable than that provided for under the terms, limitations and conditions agreed and specified in its Schedule."[69] Market access is thus limited to the commitments made by each Member according to its individual policy and economic objectives. Article XVI (2) lists the possible limitations that a Member may maintain or adopt, if specified in its Schedule, for the sectors where commitments are undertaken. These comprise limitations on number of suppliers, total value of transactions, number of operations, number of natural persons employed, participation of foreign capital, or restrictions on permitted types of legal entity.[70]

Article XVII enshrines the national treatment principle (NT), which requires Members to "accord to services and service suppliers of any other Member (…) treatment no less favorable than that it accords to its own like services and service suppliers."[71] As with market access, this obligation is limited to the sectors and modes included in the Member's Schedules, and subject to the conditions and limitations set out therein.

---

[67] *Id.* at Article I(2).
[68] Susannah Hodson, *Applying WTO and FTA Disciplines to Data Localization Measures*, 18:4 WORLD TRADE REVIEW 579, 590-92 (2019).
[69] GATS, *supra* note 58, at Article XVI(1).
[70] *Id.* at Article XVI (2) (a)–(f).
[71] *Id.* at Article XVII.

B. Assessing the GATS-Consistency of Data Regulations

Regulations on cross-border data transfers might fall under the GATS framework in different ways.[72] For instance, technologies relying on data transfers may enable other categories of covered services,[73] such as international electronic payment services or other services, not necessarily digital, that can be provided electronically across borders.[74] Moreover, data-related services such as database and data processing services may be specifically disciplined in Members' schedules and thus be subject to market access and national treatment commitments,[75] although the appropriateness of the GATS classification scheme to newer digital services is disputed.[76] Further, the GATS exceptions language is found in new-generation FTAs liberalizing trade in services,[77] which keeps WTO law and caselaw relevant to assess the legality of cross-border data flow regulations under newer instruments.

The GATS-consistency of a restriction on cross-border data flows restriction could be called into question based on different grounds.

---

[72] Crosby, *supra* note 1, at 3-4; Hodson, *supra* note 68, at 586; Susan Ariel Aaronson & Patrick Leblond, *Another Digital Divide: The Rise of Data Realms and its Implications for the WTO*, 21 J. INT'L ECON. L. 245, 251-53 (2018).

[73] Hodson, *supra* note 68, at 586-88.

[74] Mattoo & Meltzer, *supra* note 19, at 16.

[75] Crosby, *supra* note 1, at 5-6.

[76] *See* Mitchell & Hepburn, *supra* note 56, at 197-99; Hodson, *supra* note 68, at 581-82; Mira Burri, *The Regulation of Data Flows through Trade Agreements*, 48(1) GEO. J. INT'L L. 407, 410-17 (2017).

[77] *See, e.g.,* Agreement between the United States of America, the United Mexican States, and Canada (USMCA), Article 32.1.2 (Dec. 13, 2019), https://ustr.gov/trade-agreements/free-trade-agreements/united-states-mexico-canada-agreement/agreement-between (incorporating by reference); Comprehensive and Progressive Agreement for Trans-Pacific Partnership (CPTPP), Article 29.1.3, Mar. 8, 2018, https://www.international.gc.ca/trade-commerce/trade-agreements-accords-commerciaux/agr-acc/cptpp-ptpgp/text-texte/index.aspx?lang=eng (incorporating by reference); Comprehensive Economic and Trade Agreement (CETA) between Canada, of the one part, and the European Union and its Member States, of the other part, Article 28.3.2 (Oct. 30, 2016, 2017) O.J. (L 11) 23 (EU) (replicating Article XIV textually).

First, a measure could be alleged to breach a country's market access or national treatment obligations. In that case, the assessment would require analyzing the country's Schedule of Specific Commitments. The restriction would need to be applied consistent with the commitments undertaken by that country — including any specified limitations and conditions regarding the affected sectors and modes of supply. In terms of the covered modes, cross-border data flow restrictions of the type reviewed above may impact the supply of services under Modes 1 (cross-border), 2 (consumption abroad), or 3 (commercial presence). As for the affected services, there exist restrictions on data transfers for individual sectors such as banking or health; these types of regulations may be foreseen in a country's schedule.

However, the more recent privacy-oriented restrictions are of such broad scope that they may potentially affect all services that rely on data transfers. There is skepticism that a horizontal, sector-blind measure targeting cross-border data flows could be consistent with any country's GATS schedule.[78] To the extent that it remains technically possible, suffice to say that if a measure were found to be in accordance with the country's schedule, the legality analysis would end there.

Second, a measure could be alleged to breach a country's general obligations. A restriction on cross-border data transfers could result in a trade partner receiving more favorable treatment than others. For example, if data transfers to a country's territory or involving companies subject to its jurisdiction are allowed while those involving other countries are not, or if they are permitted in more convenient conditions or subject to fewer restrictions, a prejudiced country could allege a violation of MFN (Article II).

In this case, the legality of a more favorable treatment accorded to one or more countries as compared to others could be justified if it is established through a preferential trade agreement that complies with Article V, including the notification requirements.[79] But absent a treaty-based ground to grant preferential treatment to some Members

---

[78] *See, e.g.,* Nivedita Sen, *Understanding the Role of the WTO in International Data Flows: Taking the Liberalization or the Regulatory Autonomy Path?*, 21 J. INT'L ECON. L. 323, 346 (2018).

[79] GATS, *supra* note 58, at Article V(7).

to the detriment of others, a country would have to justify its measure as permitted by the General Exceptions, which will be analyzed in the next section.

C. GATS General Exceptions

This section addresses the most likely ground for discussion regarding the WTO-consistency of a cross-border data flows restriction. When a measure cannot be justified as consistent with the country's specific commitments or as falling under an exception to the MFN obligation, the ultimate line of argumentation on its WTO-consistency will turn upon its justifiability under the GATS General Exceptions,[80] and particularly the strict requirements of the necessity test and the chapeau.

GATS Article XIV, closely modeled on GATT Article XX, sets forth the general exceptions that Members can rely on to depart from their obligations *vis-à-vis* other Members and their service providers. Although there have been very few cases before the WTO Dispute Settlement Body (DSB) involving Article XIV, the Appellate Body has established that the jurisprudence on GATT Article XX is relevant to the interpretation and application of its GATS equivalent.[81]

Article XIV, like the GATT clause, provides for a two-tier analysis by a Panel. The first part consists of establishing if the measure falls within the scope of one of the exceptions. This means that the measure must address one of the listed objectives and there must be a sufficient "nexus" or connection between the measure and the interest to be protected. This nexus is required by the language of the exceptions through terms like "necessary to" and "relating to," and is thus identified as the necessity test. If the necessity test is fulfilled, the second part of the analysis consists of determining if the measure complies with the requirements of the chapeau of Article XIV.[82]

---

[80] Andrew D. Mitchell & Neha Mishra, *Regulating Cross-Border Data Flows in a Data-Driven World: How WTO Law Can Contribute*, 22 J. INT'L ECON. L. 389, 397-402 (2019); Mishra, *supra* note 1, at 9-10.

[81] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶291, WTO Doc. WT/DS285/AB/R (adopted Apr. 20, 2005) [hereinafter US - Gambling Appellate Body Report]; MATSUSHITA, ET AL, *supra* note 59, at 613-15.

[82] US - Gambling Appellate Body Report, *supra* note 81, at ¶ 292.

i. Public Interests

Beginning with the listed exceptions, the two most relevant for the purposes of data flows regulations are found in subparagraphs (a) and (c).[83]

Article XIV(a) allows for measures "necessary to protect public morals or to maintain public order."[84] As stated by the DSB, the meaning of public morals and public order may vary depending on a range of factors, and each Member enjoys broad discretion to determine the level of protection it considers appropriate.[85] However, footnote 5 to the subparagraph clarifies that public order "may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society."[86] This indicates a very high bar for justification under the public order exception as a country would need to demonstrate that a data transfer restriction seeks to address a genuine and serious threat to a fundamental interest. Conversely, the public morals language appears to preserve a larger regulatory space, and it would seem like a plausible ground to invoke to justify a privacy regulation. As for the different approaches to data transfer regulations protecting privacy, neither seems to fare better than the other under Article XIV(a) since both adequacy and accountability models seek to ensure a certain level of protection identified by the adopting country.

Article XIV(c) allows Members to adopt measures "necessary to secure compliance with laws or regulations which are not inconsistent with [the GATS]."[87] For this exception, the DSB has applied the approach adopted regarding GATT Article XX(d), which consists of three steps. A Member must identify the laws or regulations which the challenged measure is intended to secure compliance with; then it must prove that those laws or regulations are not inconsistent

---

[83] Hodson, *supra* note 68, at 593.
[84] GATS, *supra* note 58, at Article XIV(a).
[85] Panel Report, *United States—Measures Affecting the Cross-Border Supply of Gambling and Betting Services,* ¶6.461, WTO Doc. WT/DS285/R (adopted Apr. 20, 2005).
[86] GATS, *supra* note 58, Article XIV(a), footnote 5.
[87] *Id.* at Article XIV(c)(ii).

with the GATS; and demonstrate that the measure is designed to secure compliance with those laws or regulations.[88]

The exception includes a non-exhaustive list of policy objectives that the laws or regulations may pursue. Most importantly, (c)(ii) addresses "the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts."[89] This language offers the most appropriate ground for a country to justify a privacy-based restriction on cross-border data flows; of course, it would need to identify the substantive protections that the restriction advances, prove that they are themselves GATS-consistent, and demonstrate the nexus between the restriction and the substantive protections. For example, justifying the GDPR restrictions on data transfers under (c)(ii) would require identifying the substantive protections and rights enshrined therein, showing their GATS-consistency, and establishing the link between such protections and the transfer restrictions.

Like with public morals, the wording of this exception does not seem to favor any privacy approach over the other. Both adequacy and accountability models seek to ensure that personal data are subject to a certain substantive protection established in the national laws or regulations or other instruments, while the differences arise regarding the focus of such responsibility.

In any case, privacy and public morals are likely to be accepted as justifications considering the treaty language,[90] and thus a measure would be easily found to fall under subparagraphs (a) or (c). The biggest hurdles will appear in the necessity and the chapeau parts of the analysis.

ii. Necessity

Having determined that a measure falls under one of the Article XIV exceptions, the respondent Member must demonstrate that

---

[88] Panel Report, *Argentina - Measures Relating to Trade in Goods and Services*, ¶¶7.595-7.596, WTO Doc. WT/DS453/R (adopted May 9, 2016) [hereinafter Argentina–Financial Services Panel Report].
[89] GATS, *supra* note 58, at Article XIV(c)(ii).
[90] Mitchell & Hepburn, *supra* note 56, at 202-03.

the measure is "necessary to" achieve the stated objective. The DSB has established this requirement as a high threshold for respondent countries, significantly closer to the level of "indispensable" than to that of just "making a contribution to."[91] This standard demands a strong connection between the measure and the protected interest, which must be established through the "necessity test," a holistic evaluation that involves "weighing and balancing a series of factors."[92]

Although the DSB caselaw does not establish an exhaustive series of factors to be considered, the process of weighing and balancing generally involves assessing the relative importance of the interests or objectives underlying the measure; the contribution of the measure to the realization of the objective; and the restrictive impact of the measure on international trade.[93] Although the standard of necessity is objective, a Member's characterization of the measure's objectives and its regulatory approach are considered relevant to the evaluation.[94] The elements of contribution and trade-restrictiveness present the more challenging questions: the stronger the contribution of a measure to its objective, the greater trade-restrictiveness is likely to be tolerated; and the more trade-restrictive a measure, the greater the contribution to the objective that the Member must demonstrate.[95]

The final part of the necessity test consists of determining whether there exists a less trade-restrictive alternative measure that is reasonably available to the Member.[96] This requires a comparison between the measure and possible alternatives, with the burden of proof falling on the complaining Member to put forward the latter.[97] An alternative measure would not be considered reasonably available if it is merely theoretical, for example if the Member is not capable of taking it, or if it imposes an undue burden on the Member, such as prohibitive costs or substantial technical difficulties.[98] Moreover, a reasonably available alternative measure must be able to preserve the

---

[91] MacDonald & Streatfeild, *supra* note 1, at 639-40.
[92] US-Gambling Appellate Body Report, *supra* note 81, at ¶¶ 306–07.
[93] *Id.* at ¶¶ 306–07; MATSUSHITA, ET AL, *supra* note 59, at 615-17.
[94] US-Gambling Appellate Body Report, *supra* note 81, at ¶ 304.
[95] Mitchell, & Hepburn, *supra* note 56, at 204.
[96] US-Gambling Appellate Body Report, *supra* note 81, at ¶¶ 304-05.
[97] *Id*. at ¶¶ 309–10.
[98] Hodson, *supra* note 68, at 594.

right of a Member to achieve its desired level of protection regarding the objective pursued.[99]

This stage of the analysis presents the bigger challenges when assessing privacy-based restrictions. Among the factors indicated for weighing and balancing, the objectives underlying the measure will generally point to the country's identification of its public policy interests. Since Article XIV expressly mentions public morals and privacy, the necessity analysis would focus on the measure's contribution to the stated objective, its trade-restrictive impact, and the availability of alternative measures.

Here, countries enforcing strict restrictions like local storage or processing requirements, which are expected to have a highly restrictive impact on trade, will face a high burden to demonstrate the measure's contribution to the stated objective. Indeed, it has been suggested that data localization measures in themselves may not improve security or privacy, and thus may not meet the necessity test.[100] Moreover, possible alternative measures that have a less restrictive impact have been suggested, although their availability would depend on the country's technical resources.[101]

Conditional restrictions protecting privacy, however, are in a grayer area. Among the two representative approaches to cross-border data regulations (adequacy and accountability), it does not seem as either would be *per se* easier to justify under this test than the other. In any case, a respondent country would need to demonstrate that the measure contributes to data protection in a way that is proportional to the trade-restrictive impact, and there is not one particular regulatory approach that implies in itself a greater contribution to privacy or a deeper impact on trade. Assessing any individual measure would require a close analysis of the legal instrument and its actual impact, which might be technically challenging.

Further, the very existence of different regulatory approaches, and the coexistence of elements from both approaches within several individual regimes, would suggest the availability of alternative measures. The evaluation and comparison of each type of measure's trade impact and availability to a country is an exercise that the DSB,

---

[99] US-Gambling Appellate Body Report, *supra* note 81, at ¶ 308.
[100] Sen, *supra* note 78, at 337.
[101] Mitchell & Hepburn, *supra* note 56, at 204.

and even the parties to a dispute, might not be technically prepared to engage in.

This serves to illustrate that the necessity test implies a level of examination and analysis that could call any regime into question. The success of any questioned country's defense under this test will hinge on its ability to justify its regulatory choices and show that no less restrictive measure could achieve the same objective. Even considering that a measure satisfies the necessity test, it would still have to meet the chapeau requirements, which might constitute the biggest hurdle for an Article XIV defense.

iii. Chapeau

If the necessity test is passed, the last part of the analysis will be determining if the measure complies with the Article XIV chapeau. The chapeau, phrased in very similar terms to GATT Article XX, requires that the measures "are not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services."[102]

This text bars three types of effects that may arise from the application of a measure: arbitrary discrimination between countries with like conditions, unjustifiable discrimination between countries with like conditions, or a disguised restriction on trade in services. In GATT disputes, arbitrary and unjustifiable discrimination have generally been addressed together; if there is either arbitrary or unjustifiable discrimination between countries or a disguised trade restriction, the conclusion is that the measure cannot be justified under the provision.[103]

Moreover, the DSB has highlighted the use of the word "applied," suggesting that the focus of the analysis should be on how a measure is implemented and operates in practice.[104] Any arbitrariness or discrimination in the application of the measure will thus make its justification under the chapeau more difficult. For

---

[102] GATS, *supra* note 58, at Article XIV.
[103] Argentina–Financial Services Panel Report, *supra* note 88, at ¶¶ 7.745-7.746.
[104] Mitchell & Hepburn, *supra* note 56, at 204-05; MATSUSHITA, ET AL, *supra* note 59, at 620-21.

example, if data transfers are allowed to particular countries or by particular companies without the fulfilment of requirements that are imposed on others, or a set of legal standards is not applied consistently among countries, justification under the chapeau would be problematic. Moreover, arbitrariness, discrimination or a disguised restriction could be established if national service providers are exempt from prohibitions that prevent or limit data transfers by foreign companies.

Here, some distinction might be drawn between the chances for success of the two leading privacy approaches. Of course, any measure would have to be analyzed individually in terms of its application and effect. However, the respective regulatory approaches of the adequacy and accountability models present differences that might help predict which type of model could be more likely to be found in violation of the chapeau. The adequacy approach conditions data transfers upon the recipient country's privacy protections, while the accountability approach focuses on the responsible company committing to protect the data according to specified standards.

As such, adequacy determinations involve one country's decision regarding another's legal regime and can result in a ban of transfers to a country deemed to provide "inadequate" protection, or at least an additional cost for companies needing to adjust their operations to abide by any applicable safeguards. In that case, a respondent country would be obliged to demonstrate that the criteria for an adequacy determination are not applied arbitrarily or in a discriminatory manner, overcoming any suspicions about political motivations.[105]

Accountability models, on the other hand, are generally implemented as requirements in abstract that all companies must comply with regardless of their nationality. Although there could be arbitrariness, discrimination, or a disguised restriction aimed at particular companies, for example to benefit a local firm, the

---

[105] *See* Gianpaolo M. Ruotolo, *The EU data protection regime and the multilateral trading system: Where dream and day unite*, 51 QIL 5, 25-28 (2018), *and* Stefano N. Saluzzo, *Cross Border Data Flows and International Trade Law. The Relationship between EU Data Protection Law and the GATS*, XXXI(4) DIRITTO DEL COMMERCIO INTERNAZIONALE 807, 828 (2017) (suggesting that the GDPR might be incompatible with the chapeau).

regulatory approach is less likely to be used against a particular country.

Furthermore, it seems a more plausible scenario for a country to bring a complaint before the DSB against another Member's measure barring all transfers to its territory due to its "inadequacy" than to do so out of a refusal to recognize as valid an individual company's binding corporate rules or contractual arrangements.

V. CONCLUSION

This paper has explored the linkage between cross-border data flow regulations aimed at protecting privacy and the multilateral trade regime. These two spheres of regulation are growing closer as data transfers, and especially those involving personal data, become ever more central to the global economy. It is thus a matter of time before legal challenges to regulations that are perceived to disguise protectionism or discrimination against countries or firms are brought before international dispute settlement fora.

In this sense, the paper has established that privacy-based restrictions may be challenged under the GATS. Should that happen, respondent countries would be forced to justify their measures either as permitted by their GATS obligations or as covered by an exception. In the first case, a measure could be justified if it is covered by a respondent's specific commitments, which seems unlikely for a horizontal measure targeting all sectors. Otherwise, a challenge invoking a breach of MFN treatment could be survived if a "more favorable" treatment regarding data transfers were arranged through an FTA covered by Article V.

As for the GATS exceptions, privacy-based restrictions are likely to fall within Article XIV(a) or (c), but a respondent country would face a very high threshold to pass the necessity test and demonstrate compliance with the Article XIV chapeau. Regarding the latter, adequacy regimes could be especially difficult to justify if they are applied in a way that discriminates against certain countries (i.e., if adequacy determinations are granted or refused based on grounds that cannot survive the chapeau requirements). It remains to be seen whether the harmful effects of a particular restriction could be sufficiently quantifiable, or the discriminatory treatment sufficiently

demonstrable, for a country to bring suit before the WTO Dispute Settlement Body or other fora.

In any case, the implications for trade and privacy are vast and wide-ranging. With digital trade at center stage, data flows are crucial to the global economy. At the same time, countries concerned with protecting public policy interests affected by data flows, such as privacy, engage in domestic regulation with potentially significant trade implications. The international trade regime provides binding dispute settlement mechanisms offering a unique way for affected countries to bring claims against data regulations. By assessing the hurdles for justification of privacy-based restrictions under WTO law, this paper shows how the trade arena may shape the regulation of privacy in years to come. If litigation over such restrictions results in specific features of privacy regulations being considered inconsistent with WTO obligations, countries may be incentivized to make adjustments in order to avoid complaints. Moreover, WTO negotiations on electronic commerce or digital services would very likely deal with disciplines on privacy regulations, which would have to be able to pass muster under the GATS exceptions framework.

Even considering the WTO's delay in achieving new rules and the current situation at the Appellate Body, which could render WTO dispute settlement ineffective, the potential GATS-inconsistency of data regulations is also relevant to new-generation FTAs. With FTAs replicating the GATS exceptions language, binding dispute settlement under these newer instruments might also contribute to shaping privacy law by the application of the necessity analysis or by "importing" a potential WTO caselaw on the matter.

In short, this paper highlights the inextricable link between the fields of trade and privacy. Cross-border data flow regulations protecting privacy necessarily have implications for international trade. At the same time, the trade regime involves rules that, if disputed and applied, might end up invalidating some of these regulations. As this paper has shown, the ultimate line of argumentation for a country facing a complaint over a data regulation would be the GATS exceptions necessity test and chapeau requirements, and it remains to be seen whether any respondent country could win the day.