DON'T FENCE ME IN: REFORMING TRADE AND INVESTMENT LAW TO BETTER FACILITATE CROSS-BORDER DATA TRANSFER*

Andrew D. Mitchell† & Jarrod Hepburn‡
19 YALE J. L. & TECH. 182 (2017)

ABSTRACT

The transfer of data across borders supports trade in most service industries around the world as well as the growth of traditional manufacturing sectors. However, several countries have begun to adopt laws impeding the cross-border transfer of data, ostensibly in pursuit of policy objectives such as national security, public morals or public order, and privacy. Such domestic measures create potential concerns under both international trade law and international investment law. Accordingly, recent trade and investment negotiations such as the Trans-Pacific Partnership Agreement *(TPP) include specific provisions mandating the permissibility of cross-border data transfer and prohibiting data localization in certain circumstances. Although World Trade Organization law contains no such specific provisions, restrictive data transfer measures could breach the non-discrimination and market access disciplines under the* General Agreement on Trade in Services *(GATS), except to the extent that they are justified under the general exception in GATS art. XIV. International investment law may also apply to measures restricting data transfer, particularly if investment arbitrators take into account holistic changes in the digital economy to interpret the scope of covered investments and the meaning of investment obligations. The application of general trade and investment law disciplines to data transfer restrictions and localization requirements*

---

* The authors would like to thank Neha Mishra for her extensive research assistance, Jane Kluske for helpful research assistance and comments in the initial stages, Gary Horlick and Tania Voon for their insights, and the participants of the 'Regulating Cross-Border Transfer of Data' conference held at the Faculty of Law, University of Basel on 7 April 2016 for their comments. This independent research was supported by the Australian Research Council pursuant to the Future Fellowship scheme (project number FT130100416).

† Professor, Melbourne Law School, University of Melbourne; Future Fellow, Australian Research Council; Director, Global Economic Law Network; Visiting Fellow, Clare Hall and Lauterpacht Centre for International Law, University of Cambridge; PhD (Cantab); LLM (Harv); Grad Dip Int Law, LLB (Hons), BCom (Hons). (Melb).

‡ McKenzie Postdoctoral Fellow, Melbourne Law School, University of Melbourne; DPhil, MPhil, BCL (Oxon); LLB (Hons), BE(SoftEng) (Hons) (Melb).

remain uncertain. The more specific provisions in the TPP, while welcome, fail to address this uncertainty. These fields must be better synchronized with each other in respect of data transfer and with the realities of the digital economy. A comprehensive legal framework—including coverage of trade and investment law—and extensive policy coordination across a variety of stakeholders would better enable open, secure and efficient data flows across borders.

TABLE OF CONTENTS

I Introduction 185
II Restrictions on Cross-Border Data Transfers and their Underlying Rationales 188
A Storing Data Locally to Protect National Security 188
B Preventing Access to Certain Online Content to Protect Public Morals or Public Order 190
C Data Transfer Restrictions to Protect Privacy: EU-US Safe Harbor and Privacy Shield 192
III Data Flows under International Trade Law . 195
A Uncertain Application of WTO Law to Restrictions on Cross-Border Data Transfer 196
1 Problematic Classification under GATS: Mode of Supply and Sector 197
2 Most-Favored-Nation Treatment (GATS Art II): Preferential Treatment 199
3 Domestic Regulation (GATS Art VI): Burdensome Privacy-Based Requirements 199
4 Market Access (GATS Art XVI): The Problem of Zero Quotas 200
5 General Exceptions (GATS Art XIV): Central to WTO-Consistency 201
6 National Security Exceptions (GATS Art XIVbis): Limited Relevance 205
7 Conclusion 206
B Remaining Gaps in TPP Provisions on Cross-Border Data Transfer 207
1 Scope of Chapter 14 and Underlying Rationale 207
2 Parties Shall Allow Cross-Border Data Transfer (TPP Art 14.11) 208
3 Parties Shall Not Require Local Computing Facilities (TPP Art 14.13) 210
4 Exclusion of Financial Institutions from TPP Arts 14.11 and 14.13 211
5 Legal Framework for Protecting Personal Information (TPP Art 14.8) 211

6 Conclusion 214
C Developments in TTIP and TiSA: EU Position Precludes Data Flow Provisions 214

IV Data Flows under International Investment Law 216
A Threshold Requirements: Complicated But Likely Met 217
1 Existence of an 'Investment' under the ICSID Convention and the IIA 217
2 Investment "in the Territory of the Host State" 218
B Core Obligations: No Obvious Breach But Case-Dependent 221
1 No Indirect Expropriation 221
2 Fair and Equitable Treatment 223
3 Non-Discrimination 224
C Key Exceptions 225
1 General Exceptions: More Restricted Than in the Trade Context 225
2 Exceptions for National Security: Rare and Uncertain Application to Data Transfer 226
3 The Customary Defense of Necessity: A High Threshold 228
D Specific Rules on Data Transfer in the TPP: Inapplicable 229

V Reforming Trade and Investment Law to Facilitate Data Transfers: Normative Issues and Policy Options 230
A Internal Engagement: Creating Synergies in Trade and Investment Disciplines 231
B External Engagement: Achieving Coherence with Other Disciplines 234

VI Conclusion 236

I INTRODUCTION

The unprecedented growth of digital information has resulted in the expansion of new-age business models that rely on the ability to collect, aggregate, process, and transfer information across borders via the Internet to generate revenues and new business opportunities. [1] The rapid development of the Internet as a business platform has thus led to significant increases in international trade,[2] innovation,[3] and business productivity, as data transfer capabilities help reduce transaction costs and enhance real-time resource management.[4] Importantly, cross-border data flows add value not only to services and e-commerce industries, but also to manufacturing. A study by McKinsey Global Institute in 2011 found that 75% of the value added by the Internet goes to the traditional manufacturing sector. [5] Another study by the McKinsey Global Institute in 2016 estimated that all forms of global flows (such as goods, services and capital flows) increased global GDP by at least 10% (which amounted to USD 7.8 trillion), of which Internet data flows made up USD 2.8 trillion.[6] These figures highlight the broad economic potential of the Internet as a business platform for many aspects of international trade and foreign investment.[7]

---

1 Avi Goldfarb & Catherine Tucker, *Privacy and Innovation,* 12 Innovation Pol'y & Econ. 65, 83-84 (2012).

2 JOSHUA P. MELTZER, THE IMPORTANCE OF THE INTERNET AND TRANSATLANTIC DATA FLOWS FOR U.S. AND EU TRADE AND INVESTMENT 7 (2014); SUSAN STONE SUSAN, JAMES MESSENT & DOROTHEE FLAIG, EMERGING POLICY ISSUES: LOCALISATION BARRIERS TO TRADE (2015). U.S.

3 SOFTWARE & INDUSTRY INFORMATION ASSOCIATION, DATA-DRIVEN INNOVATION: A GUIDE FOR POLICYMAKERS: UNDERSTANDING AND ENABLING ECONOMIC AND SOCIAL VALUE OF DATA (2013). http://archive.siia.net/index.php?option=com_docman&task=doc_view&gid=4268&Itemid=318.

4 JOSHUA P. MELTZER, SUPPORTING THE INTERNET AS A PLATFORM FOR INTERNATIONAL TRADE 1 (2014) [hereinafter SUPPORTING THE INTERNET]; Joshua P. Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2 *Asia & the Pacific Pol'y Studies* 90, 92 (2014) [hereinafter THE INTERNET, CROSS-BORDER DATA FLOWS]; UNITED STATES INTERNATIONAL TRADE COMMISSION, DIGITAL TRADE IN THE U.S, AND GLOBAL ECONOMIES, PART 2 65 (2014). U.S.

5 MATTHIEU PÉLISSIÉ DU RAUSAS, JAMES MANYIKA, ERIC HAZAN, JACQUES BUGHIN, MICHAEL CHUI & RÉMI SAID, INTERNET MATTERS: THE NET'S SWEEPING IMPACT ON GROWTH, JOBS, AND PROSPERITY 1 (2011)., http://www.mckinsey.com/insights/high_tech_telecoms_internet/internet_matters.

6 JAMES MANYIKA, SUSAN LUND, JACQUES BUGHIN, JONATHAN WOETZEL, KALIN STAMENOV & DHRUV DHINGRA, DIGITAL GLOBALIZATION: THE NEW ERA OF GLOBAL FLOWS 1 (2016); *See also* UNITED NATIONS CONFERENCE ON TRADE AND DEVELOPMENT, DATA PROTECTION REGULATIONS AND INTERNATIONAL DATA FLOWS: IMPLICATIONS FOR TRADE AND DEVELOPMENT xi (2016).

7 SUPPORTING THE INTERNET, *supra* note 4, at vi.

Although international data transfer assists both businesses and consumers, while generating benefits for the economy at large, several countries (both developing and developed) have imposed restrictions on the cross-border flow of data.[8] The proffered justifications for such restrictions include policy concerns like safeguarding privacy and security,[9] but digital protectionism may also be at play,[10] entailing for example the promotion of the local information and communications technology industry either directly by providing preferential treatment in government procurement to domestic cloud computing companies, or indirectly by coercing foreign companies to locate their servers domestically. These restrictions tend to reduce market access for foreign suppliers of digital services, impeding trade and investment opportunities and increasing the costs and service choice of individual businesses.[11]

The need to facilitate data transfer is a global concern,[12] but few specific rules on data transfer (or data protection) exist at the international level. Meltzer has proposed the World Trade Organization (WTO) as a forum for developing the necessary rules, for example by expanding WTO Members' commitments under the *General Agreement on Trade in Services* (GATS)[13] to cover the scope of online trade.[14] However, even with regard to specific commercial aspects such as e-commerce, discussions within the WTO have been marginal, with more high-profile discussion of the digital economy occurring within the human rights institutions.[15] More progress has been made at plurilateral rather than multilateral levels, with the new wave of mega-regional agreements

---

8 These include developed countries in the EU and Australia and Korea, as well as developing countries such as China, India, Indonesia, Vietnam, Nigeria and Russia.

9 *See generally* CHRISTOPHER KUNER, REGULATION OF TRANSBORDER DATA FLOWS UNDER DATA PROTECTION AND PRIVACY LAW: PAST, PRESENT AND FUTURE (2011).

10 Shahmel Azmeh & Christopher Foster, *The TPP and the digital trade agenda: Digital industrial policy and Silicon Valley's influence on new trade agreements* 11 (LSE International Development, Working Paper No. 16-175, 2016).

11 *Cross-Border Data Flows: Could Foreign Protectionism Hurt U.S. Jobs? Hearing before the Subcomm. on Commerce, Mfg., and Trade of the Comm. on Energy and Commerce, H. of Rep., 113th Cong.,* 8 (2015) (statement of Linda Dempsey, Vice President of International Economic Affairs, National Association of Manufacturers).

12 Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 *EUR. J. OF INT'L L.* 441, 456 (2010).

13 Marrakesh Agreement Establishing the World Trade Organization annex 1B, *opened for signature* 15 April 1994, 1869 U.N.T.S. 183.

14 THE INTERNET, CROSS-BORDER DATA FLOWS, *supra* note 4, at 99.

15 Julian Braithwaite, Ambassador and Permanent Representative, UK Mission to the UN and Other Int'l Org., Discussion at the Trade and Development Symposium (16 December 2015).

containing specific obligations related to cross-border data flow. For example, the final text of the *Trans-Pacific Partnership Agreement* (TPP),[16] signed by 12 countries in February 2016, contains such provisions, which have also been proposed in the ongoing negotiations towards the *Trade in Services Agreement* (TiSA) [17] and the *Transatlantic Trade and Investment Partnership* (TTIP).[18]

In this article, we argue that existing rules of international trade and investment law do not protect cross-border data transfer in a consistent, coherent and predictable manner. In part II, we explain the types of data restrictions that countries have implemented in recent years and the most common rationales put forward by such countries for these restrictions. We highlight the impossibility of characterizing a given measure as lawful or unlawful, legitimate or illegitimate, purely on the basis of its ostensible rationale. In part III, we investigate how such restrictions are currently addressed in international trade law (focusing on the WTO and the TPP), concluding that restrictions on cross-border data transfer may give rise to a number of potential violations, save for the availability of specific exceptions subject to stringent conditions. The application of the general WTO rules is uncertain. The specific provisions in the TPP, while more directed, reflect a failure to achieve consensus even among a limited number of countries on the necessary balance between free flow of data and recognition of other policy objectives.

In part IV, we show that threshold requirements in a typical investment treaty, of an "investment" "in the territory of the host state", are likely to be satisfied in respect of businesses engaging in cross-border data transfer, despite some complications with their business models in comparison to more traditional industries. However, restrictions on cross-border data transfer will not necessarily amount to violations

---

16 Trans-Pacific Partnership Agreement, Feb. 4, 2016, http://dfat.gov.au/trade/agreements/tpp/official-documents/Pages/official-documents.aspx [hereinafter TPP].

17 The latest draft of the Annex on Electronic Commerce was leaked on May 25, 2016 by Wikileaks. *See Trade in Service Agreement: Annex on Electronic Commerce* art 2., WIKILEAKS (May 25, 2016), https://wikileads.org/tisa/document/20151001_Annex-on-Electronic-Commerce/20151001_Annex-on-Electronic-Commerce.pdf.

18 Transatlantic Trade and Investment Partnership: Proposal for Trade in Services, Investment and E-Commerce 47-50 (July 31, 2015), <http://trade.ec.europa.eu/doclib/docs/2015/july/tradoc_153669.pdf 47-50. The EU proposal does not contain any proposals related to cross-border transfer of information. In the latest draft, leaked by Greenpeace on May 1. 2016, the U.S. proposal for the provision on cross-border flow of information can be found. For more details, see *Transatlantic Trade and Investment Partnership: Consolidated Proposed Electronic Communications/Telecommunications Text* art X.10.3, TTIP-LEAKS.ORG BY GREENPEACE (last accessed on Feb. 9, 2017), https://www.ttip-leaks.org/agamemnon/doc4.pdf.

of key investment protections, even in more modern agreements providing for data transfer commitments such as the TPP.

After analyzing the present application of trade and investment law to data transfer, Part V sets out a number of normative and policy reforms that treaty-makers and adjudicators could adopt in order to facilitate freer cross-border transfer of data. Part V observes that better coordination is needed between international trade and investment law with respect to data transfer, and also between trade and investment laws on the one hand and the realities of the digital economy on the other. Open, secure, and efficient data flows across borders require a comprehensive legal framework, including trade and investment law disciplines, as well as extensive policy coordination across a variety of stakeholders. Part V thus proposes a dual-pronged strategy of internal and external engagement to achieve this coordination and to secure the future of cross-border data transfer.

II RESTRICTIONS ON CROSS-BORDER DATA TRANSFERS AND THEIR UNDERLYING RATIONALES

A number of governments have established restrictions on cross-border data transfer, particularly in recent years, offering various legitimate policy objectives as justifications. Before turning to an assessment of these restrictions under international trade and investment law, we explore these objectives and their relationship to the restrictions undertaken. As with many regulations, the difficulty is in distinguishing the protectionist aspects of data transfer restrictions from genuine policy objectives unrelated to trade and investment. The following brief review demonstrates that the dividing line between legitimate regulation and protectionist intervention must be drawn on a case-by-case basis and that reasonable arguments may be put forward on both sides. As detailed further in parts III and IV below, the specific crafting of the challenged measure and the language and practice of its implementation are crucial in determining its permissibility under trade and investment law.

A Storing Data Locally to Protect National Security

National security is a common rationale for restricting data transfers in a number of countries. The government procurement policies of many countries require that data related to national security and the defense sector be stored in

domestic servers.[19] Further, countries such as Russia,[20] Vietnam,[21] and Indonesia[22] view data sovereignty as a matter of national security and protection against foreign surveillance. Countries may also impose restrictions on cross-border data flows in connection with critical infrastructure sectors, particularly with respect to government data. For example, both Germany[23] and France[24] are working towards establishing local clouds for government data. Some commentators have questioned the effectiveness of such restrictions to enhance national security, arguing that foreign surveillance can still be carried out even if data is stored locally and that data may be even more vulnerable to security attacks if concentrated in a single location.[25]

---

19 On the requirement of storing sensitive information of public authorities in servers located within Germany, see Beschluss des Rates der IT-Beauftragten der Ressorts, Nr. 2015/5, July 29, 2015 (Ger.), *cited in* Matthias Bauer & Hosuk Lee-Makiyama, *The Bundes Cloud: Germany on the Edge to Discriminate against Foreign Suppliers of Digital Services*, ECIPE BULLETIN, September 2015, http://ecipe.org/publications/the-bundes-cloud-germany-on-the-edge-to-discriminate-against-foreign-suppliers-of-digital-services/. For the requirement to store all data collected with public funds in local servers in India, see MINISTRY OF SCIENCE & TECHNOLOGY, NATIONAL DATA SHARING AND ACCESSIBILITY POLICY-2012 [10] (March 17, 2012) (Ind.). For the requirement for auditing for hardware and software used in government communications in Brazil, see Decreto No. 8.135, de 4 de Novembro de 2013, Diário Oficial da União [D.O.U.] de 11.5.2013 (Braz.). *See also infra* notes 20-24.

20 Federal Law No. 242-FZ "On Amending Certain Legislative Acts of the Russian Federation for Clarification of the Procedure of Personal Data Processing in Information and Telecommunication Networks,", dated July 21, 2014, entered into force September 1, 2016.

21 Decree on the Management, Provision and Use of Internet Services and Online Information, No. 72/2013/ND-CP. art 4.4, art 5 (July 15, 2013) (Viet.).

22 Undang-Undang Tentang Pelayanan Publik [Public Service Law], Law No 25/2009, July 18, 2009 (Government Gazette of the Republic of Indonesia Year 2009 No. 112), http://www .setneg.go.id//components/com_perundangan/docviewer.php?id=2274&file name=UU%2025%20Tahun%202009.pdf. *See also* Anupam Chander & Uyen P Le, *Breaking the Web: Data Localization vs the Global Internet* 19-20 (UC Davis Legal Studies, Research Paper No 378, 2014)..

23 All cloud computing services purchased by public authorities in Germany must store sensitive information within Germany. *See* Beschluss des Rates der IT-Beauftragten der Ressorts, Nr. 2015/5, July 29, 2015 (Ger.). *See* Hosuk Lee-Makiyama & Matthias Bauer, *The Bundes Cloud: Germany on the Edge to Discriminate against Foreign Suppliers of Digital Services* ECIPE BULLETINS (September 2015), http://ecipe.org/publications/the-bundes-cloud-germany-on-the-edge-to-discriminate-against-foreign-suppliers-of-digital-services/.

24 Valery Marchive, *France Hopes to Turn PRISM Worries Into Cloud Opportunities*, ZDNET(Jun. 21, 2013), http://www.zdnet.com/article/france-hopes-to-turn-prism-worries-into-cloud-opportunities/; Valery Marchive, *Cloud Firms Demand Right to Use French Government's €285m "sovereign cloud"*, ZDNET (Feb. 5, 2013), http://www.zdnet.com/article/cloud-firms-demand-right-to-use-french-governments-eur285m-sovereign-cloud/.

25 Chander & Le, *sura* note 22, at 30.

B Preventing Access to Certain Online Content to Protect Public Morals or Public Order

The 'Great Firewall' in China[26] (coupled with highly restrictive domestic regulations on cross-border data transfer)[27] has created strong impediments to the flow of data across Chinese borders. The purpose of these Chinese laws and policies is to ensure that all online content that is circulated within China is in line with important public values, particularly pertaining to maintaining public order and protecting the nation's public morals.[28] In 2016, the United States Trade Representative ('USTR') officially identified these restrictions as a barrier to trade in its National Trade Estimate Report.[29]

Several other countries also impose restrictions on online data transfer in particular sectors for reasons of 'public order' or 'public morals'. These restrictions may apply generally to online services or websites (whether local or international), or only to transfers from outside the country's territory. The latter type of restriction may be harder to justify on moral grounds. Countries including Singapore,[30] Lebanon[31] and Turkey[32] ban adult entertainment websites, while Germany bans the sale of Nazi memorabilia on e-commerce websites.[33]

---

26 The term "Great Firewall of China" was coined by Barme and Ye, referring to the online censorship and surveillance tools employed by the Chinese Ministry of Public Security. *See* Geremerie R. Balme & Sang Ye, *The Great Firewall of China*, WIRED (Jan. 6, 1997), https://www.wired.com/1997/06/china-3/ . *See also How Censorship Works in China: A Brief Overview*, HUMAN RIGHTS WATCH, https://www.hrw.org/reports/2006/china0806/3.htm (last visited Feb. 6, 2017).

27 *See, e.g.*, 信息安全技术公共及商用服务信息系统个人信息保护指南[Information Security Technology – Guidelines for Personal Information Protection Within Public and Commercial Services Information Systems] (effective Feb. 1, 2013) (China); *Cybersecurity Law (Draft) (Second Reading Draft*), CHINA LAW TRANSLATE (April 7, 2016), http://chinalawtranslate.com/cybersecurity2/?lang=en.

28 Shi Hao, Liu Fei & Wang Jianhua, *Commentary: China's Internet Regulation Not Trade Barrier,* XINHUANET (Apr. 14, 2016), http://news.xinhuanet.com/english/2016-04/14/c_135279379.htm. *See also Computer Information Network and Internet Security, Protection and Management Regulations* art 4-6 (approved by St. Council on Dec. 11, 1997, promulgated by the Ministry of Public Security on Dec. 30, 1997) (China).

29 UNITED STATES TRADE REPRESENTATIVE, THE 2016 NATIONAL TRADE ESTIMATE REPORT 91 (2016).

30 Internet Code of Practice, art. 4 (1 November 1997) (Sing.).

31 Mohammed Najem, *Lebanon Bans Six Porn Sites, Sparks Fears of Future Censorship*, *GLOBAL VOICES* (Sept. 10, 2014,) <https://advox.globalvoices.org/2014/09/10/lebanon-blocks-six-porn-sites-sparks-fears-of-further-censorship/>.

32 Mustafa Akgül & Melih Kırlıdoğ, *Internet Censorship in Turkey*, 4 INTERNET POL'Y REV. (2015)<http://policyreview.info/articles/analysis/internet-censorship-turkey>.

33 STRAFGESETZBUCH [CRIMINAL CODE], § 86a, (Ger.).

Countries such as Iran,[34] Vietnam,[35] and China[36] impose restrictions on political information that is circulated online for the purposes of maintaining public order. Therefore, any information that may be prejudicial to 'national security', 'cultural values' or 'public order' is prohibited from online circulation. These kinds of regulations have the net effect of preventing cross-border transfer of data from foreign countries into countries where specific websites or types of content are banned. As discussed further below, the WTO Appellate Body has already decided two disputes involving challenges to restrictions on online services related to gambling and audiovisual products, in both of which the respondent (the United States ('US') and China respectively) justified the measures on the basis of public morals.[37]

The Internet has made it harder for governments to control the kind of information that their citizens can access and share. As discussed above, many countries take strong measures to prevent dissemination of information that may destabilize the government or is directed against the predominant belief system, but alternative routes still enable access to information from blocked websites/portals. For instance, citizens can access information through virtual private networks or proxy servers even in countries such as China, including obtaining access to banned websites such as Facebook within Chinese borders.[38] The existence of such

---

34 *See generally* Simburgh Aryan, Homa Aryan & J. Alex Halderman, *Internet Censorship in Iran: A First Look*, *in* PROCEEDINGS OF THE 3RD USENIX WORKSHOP ON FREE AND OPEN COMMUNICATIONS ON THE INTERNET, (Aug. 2013).

35 Decree on the Management, Provision and Use of Internet Services and Online Information, No. 72/2013/ND-CP. art 4.4, art 5 (July 15, 2013) (Viet.); Eva Galperin & Maira Sutton, *Vietnam Internet Censorship Bill Goes Into Effect,* ELECTRONIC FRONTIER FOUND (Sept. 10, 2013), <https://www.eff.org/deeplinks/2013/09/vietnams-internet-censorship-bill-goes-effect>.

36 *Computer Information Network and Internet Security, Protection and Management Regulations* art 4-6 (approved by St. Council on Dec. 11, 1997, promulgated by the Ministry of Public Security on Dec. 30, 1997) (China)

37 Appellate Body Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 95, 294, 296, 301, 313, WTO Doc. WT/DS285/AB/R (adopted Apr. 7, 2005) [hereinafter *U.S. — Gambling*]; Appellate Body Report, *China — Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, ¶ 141, WTO Doc. WT/DS363/AB/R (adopted Dec. 21, 2009) [hereinafter *China — Publications and Audiovisual Products*].

38 *See, e.g.*, Paul Bischoff, *5 Ways to Sneak Through China's Great Firewall*, TECH IN ASIA (Mar. 24, 2014), https://www.techinasia.com/5-ways-sneak-chinas-great-firewall; Simon Denyer, *Internet Activists are Finding Ways Around China's Great Firewall*, WASH. POST (June 14, 2016), https://www.washingtonpost.com/world/asia_pacific/the-cat-and-mouse-game-between-chinas-censors-and-internet-activists/2016/06/14/77f2b3a8-1dd9-11e6-b6e0-c53b7ef63b45_story.html.

technical workarounds tends to undermine the effectiveness of such bans and hence their rationale (and, perhaps, their justifiability under international economic law, as discussed further below).

C Data Transfer Restrictions to Protect Privacy: EU-US Safe Harbor and Privacy Shield

A government may feel compelled to restrict data flows in order to protect its citizens and businesses from breaches of privacy involving personal or confidential data, leading to the creation of digital walls between its territory and the rest of the world.[39] Restrictions on cross-border transfer of data are thus not unusual in sectors such as health and finance, which are particularly sensitive to privacy concerns.[40] These kinds of concerns have the potential to challenge new business models based on Big Data, which require analysis of huge datasets collected through various online services and digital applications. Big Data business models can create benefits such as projection of customer demand, customization of services and advertisements, and greater efficiency. However, Big Data processing technologies may also allow individuals to be identified by aggregating and deducing from blocks of non-personal data, usually for commercial purposes such as targeted advertising,[41] but potentially also for more problematic purposes such as political repression and surveillance. Governments have thus expressed concern over sending and storing citizens' personal information, even in aggregate form, outside their own borders.

One way around these privacy concerns has been the negotiation of bilateral agreements between particular countries that have a degree of confidence in each other's privacy regimes and benign motives. The former 'Safe Harbor' agreement between the European Union ('EU') and the U.S., for instance, represented an attempt at such an arrangement, intended to balance privacy with economic concerns. However,

---

39 JOSEPH WRIGHT, DATA RESTRICTIONS 'REGRETTABLY' ON RISE: STRICKLING, Int'l Trade Daily (Nov. 10, 2015).

40 For example, Australia restricts transfer of e-health records of its residents on grounds of protecting their privacy (*Personally Controlled Electronic Health Records Act 2012* (Cth) s 77 (Austl.)). China imposes restrictions on transferring financial information of Chinese citizens abroad for the purposes of analysis, processing and storage (中国人民银行关于银行业金融机构做好个人金融信息保护工作的通知 [Notice to Urge Banking Financial Institutions to Protect Personal Information] (promulgated by the People's Bank of China, Jan. 21, 2011, effective May 1, 2011) PEKING U. LAW, http://en.pkulaw.cn/display.aspx?cgid=187253&lib=law (China).

41 *See* Diane MacDonald & Christine Streatfeild, *Personal Data Privacy and the WTO*, 36 HOUS. J. INT'L L. 625, 644 (2014).

the agreement also highlighted a philosophical gap between the two jurisdictions with respect to privacy. While the EU considers safeguarding of personal data a human right, the U.S. sees the issue of data protection mainly in the terms of consumer protection.[42] In the European legal system, Directive 95/46/EC prohibited transfer of personal data to third countries lacking adequate data protection.[43] To facilitate data transfer between the EU and the U.S., the two sides concluded the 'Safe Harbor' agreement in 2000, allowing firms to transfer data from the EU to the U.S. if the firms self-certified that they provided safeguards equivalent to those required by the EU Directive.[44] When the Safe Harbor agreement was first signed, "the [I]nternet was in its infancy," and the transatlantic flow of data was insubstantial.[45] However, the exponential increase in data transfer[46] and high-profile data security breaches, such as Edward Snowden's leaks regarding the U.S. National Security Agency ('NSA') in 2013, led to tension between the parties.[47]

Following the NSA leaks, an Austrian privacy activist, Maximillian Schrems, raised concerns that his right to privacy was being compromised when his personal data, given to Facebook through his use of the site, was transferred to U.S.-based servers under the Safe Harbor agreement. After various proceedings in Ireland, the case was transferred to the European Court of Justice (ECJ).[48] On October 6, 2015, the ECJ decided that the Safe Harbor agreement compromised the essence of the fundamental right to respect for private life, as it

---

42 *An Ocean Apart: Online Privacy in Europe*, THE ECONOMIST ESPRESSO (Dec. 15, 2015), https://espresso.economist.com/90f6536e97bcf229cfa3dc415f5a7f64.

43 Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (L 281); Lingjie Kong, *Data Protection and Transborder Data Flow in the European and Global Context*, 21 *EUR. J. INT'L.L.* 441, 441 (2010).

44 Commission Decision 2000/520/EC, of 26 July 2000 Pursuant to Directive 95/46/EC of the European Parliament and of the Council on the Adequacy of the Protection provided by the Safe Harbour Privacy Principles and Related Frequently Asked Questions Issued by the U.S. Department of Commerce, 2000 O.J. (L 215) art. 1, 2. *U.S.*

45 *Get off of my Cloud; Data and privacy*, THE ECONOMIST 61-2 (Oct. 10, 2015).

46 "Data flows between the U.S. and the EU are the largest in the world: approximately 55 percent higher than those between the U.S. and Asia, and 40 percent higher than those between the U.S. and Latin America." Joshua P. Meltzer, *Examining the EU safe harbor decision and impacts for transatlantic data flows*, BROOKINGS (Nov. 3, 2015), <http://www.brookings.edu/research/testimony/2015/11/03-eu-safe-harbor-decision-transatlantic-data-flows-meltzer>.

47 *Get off of my Cloud; Data and privacy*, *supra* note 45.

48 Case C-362/14, *Schrems v Data Prot. Comm'r* (Oct. 6, 2015), http://curia.europa.eu/juris/document/document.jsf?docid=169195&doclang=en

enabled U.S. public authorities to have general access to the content of electronic communications.[49]

Following the invalidation of the Safe Harbor agreement by the ECJ in *Schrems v Data Protection Commissioner*, the EU and U.S. adopted a new legal framework known as the Privacy Shield,[50] which applies to 4,400 companies following its entry into force in July 2016.[51] The EU-U.S. Privacy Shield regulates the transatlantic flow of personal data,[52] imposing stronger obligations on the U.S. side than the previous Safe Harbor agreement. Nevertheless, the new agreement has also seen strong objections by EU-level bodies such as the Article 29 Working Party, [53] European Parliament,[54] and European Data Protection Supervisor, [55] and may itself be subject to legal challenge before the European courts, [56] particularly when the General Data Protection Regulation comes into force in 2018.[57]

In recent years, individual EU countries have also been imposing restrictions on cross-border data transfer. For instance, in 2016, the French Data Protection Authority fined Google for violating the so-called "right to be forgotten," relating to the processing and deletion of personal data from search engine results delivered into particular jurisdictions.[58]

---

49 *Id.* at ¶¶ 94, 78.

50 Commission Implementing Decision 2016/1250, 2016 O.J. (L 207) 1.

51 European Commission Press Release, European Commission Launches EU-U.S. Privacy Shield: Stronger Protection for Transatlantic Data Flows (July 12, 2016); Stephen Gardner, *EU Countries Green Light Data Transfer Privacy Shield*, BLOOMBERG LAW: PRIVACY AND DATA SECURITY (July 8, 2016), https://www.bna.com/eu-countries-green-n57982076798/.

52 Commission Implementing Decision 2016/1250, ¶¶14-18, 2016 O.J. (L 207) 1.

53 *See generally* Statement, Article 29 Working Party, Statement of the Article 29 Working Party on the Opinion on the EU-U.S. Privacy Shield (April 13, 2016), http://ec.europa.eu/justice/data-protection/article-29/press-material/press-release/art29_press_material/2016/press_release_shield_en.pdf.

54 Catherine Stupp, *Parliament asks Commission to renegotiate Privacy Shield*, EURACTIV (May 27, 2016), http://www.euractiv.com/section/digital/news/parliament-asks-commission-to-renegotiate-privacy-shield/.

55 *See Opinion of European Data Protection Supervisor on the EU-US Privacy Shield Draft Adequacy Decision* (May 30, 2016), <https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2016/16-05-30_Privacy_Shield_EN.pdf.>.

56 *See, e.g.*, Jack Caporal, *European Data Officials Not Satisfied with Final Privacy Shield Text*, INSIDE U.S. TRADE (July 29, 2016). *U.S.*

57 Commission Regulation 95/46, 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, 2016 (L 119) 1 (hereinafter General Data Protection Regulation).

58 Julia Fioretti, *France fines Google over 'right to be forgotten,'* Reuters (March 24, 2016), http://www.reuters.com/article/us-google-france-privacy-idUSKCN0WQ1WX.

Outside the EU, Australia[59] and certain Canadian provinces[60] have also invoked privacy as the basis for restricting cross-border data flows.

The common resort to restrictions on data transfer as a means of protecting privacy, in a number of countries, demonstrates the significance of this policy objective, despite the potential damage to international trade and investment arising from such restrictions. However, the discrepancies in approach between jurisdictions, such as between the EU and the U.S., exemplify the complexities of this area and the difficulties in reaching agreement on how such measures should be addressed in international trade and investment law.

III DATA FLOWS UNDER INTERNATIONAL TRADE LAW

The existing WTO laws largely predate the pervasive nature of data transactions today.[61] In applying WTO law to such restrictions, as we explain below in part IIIA, much depends on the specific design and implementation of the measure, its impact on trade, and its connection to relevant policy rationales. Potential difficulties arise in classifying data transfers under the broad concepts of goods and services in the WTO. The WTO does provide useful concepts and tools for analyzing some of the policy objectives associated with data transfer restrictions, particularly in the form of general exceptions (including reference to privacy,[62] public morals, and public order) and national security exceptions. However, relying solely on these overarching exceptions may have the effect of deferring international consensus on the appropriate regulation of data and data transfer, in the meantime leaving much to the discretion of WTO panels and the Appellate Body.

More modern approaches to addressing data transfer in international trade law are found in newer agreements such as the recently concluded TPP, as we outline in part IIIB below. By recognizing objectives such as consumer protection in e-

---

59 Australia restricts transfer of e-health records of its residents on grounds of protecting their privacy. *See Personally Controlled Electronic Health Records Act 2012* (Cth) s 77 (Austl.).

60 *Freedom of Information and Protection of Privacy Act*, R.S.B.C. 1996, s 30.1 (B.C.); *Personal Information International Disclosure Protection Act*, N.S. 2006, s 5 (N.S.).

61 John A. Drennan, J. Michael Taylor, Joseph Laroski, Alexander K. Haas & Julie A. Stockton, *Privacy Law, Cross-Border Data Flows and the Trans-Pacific Partnership Agreement: What Counsel Need to Know*, BLOOMBERG: PRIVACY & SECURITY LAW REPORT (14 December 7, 2015), http://www.kslaw.com/imageserver/KSPublic/library/publication/2015articles/12-07-15_Bloomberg-BNA-Privacy-and-Security-Law-Report.pdf..

62 *Id.*. *See also* ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT, OECD COUNCIL RECOMMENDATION ON PRINCIPLES FOR INTERNET POLICY MAKING (2011).

commerce, the TPP parties have enhanced possibilities for cooperation and policy coordination between themselves to ensure safe and secure cross-border transfer of data, through transparent and coherent laws on data transfer that balance digital trade liberalization with other objectives including privacy.[63] The significance of the TPP provisions for the free flow of data across borders depends, of course, on that agreement entering into force. Meanwhile, as we note in part IIIC, the EU position may prevent the inclusion of similar provisions specific to data transfer in TTIP and TiSA. Moreover, as discussed further below, even the specific TPP provisions have significant gaps that need to be filled by international standards to be developed through further coordination.

A Uncertain Application of WTO Law to Restrictions on Cross-Border Data Transfer

In the WTO, measures relating to cross-border transfer of data are most likely to be examined under the GATS,[64] because digital data is usually transferred across borders without requiring any transfer of physical commodities.[65] Other WTO agreements may also apply, such as the *Agreement on Trade-Related Aspects of Intellectual Property Rights* (TRIPS Agreement)[66] for the intellectual property invested in the data and the *General Agreement on Tariffs and Trade 1994* (GATT 1994)[67] in relation to digital goods, like software or music in electronic format embedded in a physical medium such as a

---

63 Usman Ahmed & Anupam Chander, *Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows*, 5 (E15 Expert Group on the Digital Economy, Think Piece, International Centre for Trade and Sustainable Development and World Economic Forum, Nov. 2015).

64 *See* General Agreement on Trade in Services arts I:1, XXVIII(b)., Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1B, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 284 (1999), 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994) [hereinafter GATS]. *See also* Appellate Body Report, *European Communities — Regime for the Importation, Sale and Distribution of Bananas*, ¶220, WTO Doc WT/DS27/AB/R (9 September 1997).

65 The issue of whether software embedded in a physical medium constitutes a service or a good remains unresolved in WTO law.

66 Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, THE LEGAL TEXTS: THE RESULTS OF THE URUGUAY ROUND OF MULTILATERAL TRADE NEGOTIATIONS 320 (1999), 1869 U.N.T.S. 299, 33 I.L.M. 1197 (1994) [hereinafter TRIPS Agreement].

67 General Agreement on Tariffs and Trade, Oct. 30, 1947, 61 Stat. A-11, 55 U.N.T.S. 194 [hereinafter GATT].

compact disc.[68] Here we focus on trade in services. However, similar issues may arise in the context of goods trade. For instance, many e-commerce companies that deliver goods like apparel, electronic devices, or books across borders also rely on cross-border transfer of data. Below, we first address certain classification questions before turning to the potentially applicable GATS obligations and exceptions.

1 Problematic Classification under GATS: Mode of Supply and Sector

If a WTO Member's data transfer restriction is challenged as a violation of GATS, in order to assess whether the restriction complies with the Member's applicable GATS obligations, we must first consider two classification questions: (a) the "mode" under which the data is transferred and (b) the relevant service "sector." International transfer of data via the Internet for any kind of service could be categorized as either cross-border supply (mode 1: supply of a service "from the territory of one Member into the territory of any other Member")[69] or consumption abroad[70] (mode 2: "in the territory of one Member to the service consumer of any other Member"). [71] Simultaneous classification under both modes could create difficulties in identifying the relevant commitments of the Member when the commitments for the relevant sector differ between the two modes. Thus, on one view, for the purposes of legal certainty, mode 1 classification is appropriate.[72] In U.S. — *Gambling*, the Panel and Appellate Body addressed the cross-border supply of online gambling services from Antigua to the U.S. under mode 1.[73] However, other modes may also be relevant. For example, in *China – Electronic Payment Services*, the Panel—whose report was not appealed—found that certain Chinese measures disadvantaging foreign suppliers in the provision of certain

---

68 *See, e.g.*, Peter Drahos, *Global Property Rights in Information: The Story of TRIPS at the GATT* 13 PROMETHEUS 6 (1995).

69 GATS art. 1, ¶ 2(a).

70 *See* Carla L Reyes, *WTO-Compliant Protection of Fundamental Rights: Lessons from the EU Privacy Directive*, 12 MELBOURNE J. OF INT'L L. 141, 149 (2011); SACHA WUNSCH-VINCENT, THE WTO, THE INTERNET AND TRADE IN DIGITAL PRODUCTS: EC–US PERSPECTIVES 65-70 (2006) .

71 GATS art. 1, ¶ 2(b).

72 Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitment* 3 (E15 Expert Group on the Digital Economy, Think Piece, International Centre for Trade and Sustainable Development and World Economic Forum, Mar. 2016).

73 Panel Report, *United States — Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶¶ 6.285-87, ¶6.29, WTO Doc. WT/DS285/R (Nov. 10, 2014); Appellate Body Report, *United States — Gambling, supra* note 37, at ¶ 215.

payment card transactions, which may involve data transfer, violated China's commitments under not only mode 1, but also mode 3[74] (supply of a service "by a service supplier of one Member, through commercial presence in the territory of any other Member").[75]

Identifying the relevant service sector for the purposes of GATS is also difficult.[76] A common classification approach adopted by WTO Members in their GATS schedules is the United Nations Central Product Classification (CPC),[77] but this system has not kept pace with technological developments. For example, computer services and audio-visual services can now be accessed through mobile networks.[78] Therefore, even common services such as cloud computing, cloud-based apps, and social network platforms, which are used by service suppliers across different sectors, cannot be neatly classified under computer services ("data processing services" (CPC 843) or "data base services" (CPC 844)). Other categories for classification of telecommunication services (CPC 7523, which pertains to data transmission over mobile networks) may become more relevant to such services.[79] Other contentious classification issues arise with respect to different forms of digital content that are frequently traded, such as online publishing of audio-visual services and other media products.[80] These kinds of uncertainties regarding classification may need to await clarification on a case-by-case basis as further disputes arise in this field.

The relevant service sector may also be affected by the *content* of the data being restricted. In *U.S. – Gambling*, for example, the relevant sector was 10.D: "Other recreational services (except sporting)."[81] In *China – Publications and Audiovisual Products*, the Appellate Body agreed with the Panel that sector 2.D of China's GATS schedule ("Sound recording distribution services") extended to electronic

---

74 *See, e.g.*, Panel Report, *China – Certain Measures Affecting Electronic Payment Services*, ¶ 8.1(f)(i), WTO Doc. WT/DS413/R (July 16, 2012), https://www.wto.org/english/tratop_e/dispu_e/413r_e.pdf [hereinafter *China -- Electronic Payment Services*].

75 GATS art. 1, ¶ 2(c).

76 This problem was recognized in one early paper on the issue. *See* Tim Wu, *The World Trade Law of Censorship and Internet Filtering*, 7 CHI. J. INT'L L. 263, 281–84 (2006).

77 *See, e.g.*, UNITED NATIONS STATISTICS DIVISION, CENTRAL PRODUCT CLASSIFICATION (CPC) VER. 2 (Dec. 31, 2008).

78 For more discussion, see Lee Tuthill & Martin Roy, *GATS Classification Issues for Information and Communication Technology Services*, in TRADE GOVERNANCE IN DIGITAL AGE 157, 161 (Mira Burri & Thomas Cottier eds., 2012).

79 *Id.* at 164.

80 *Id.* at 158-61.

81 *See, e.g.*, Appellate Body Report, *United States — Gambling, supra* note 37, at ¶¶ 158, 162

distribution,[82] in relation to which certain Chinese measures had restricted foreign involvement (in relation to mode 3). In *China – Electronic Payment Services*, the Panel classified services "essential to the processing and completion of transactions using payment cards" as falling within sector 7B(d): "All payment and money transmission services."[83] Thus, numerous service sectors are potentially relevant to cross-border data transfer under GATS.

2 Most-Favored-Nation Treatment (GATS Art II): Preferential Treatment

Subject to the issues of classification and relevant schedule commitments just discussed, measures relating to data transfer could implicate a range of GATS obligations. Firstly, alleviating data transfer restrictions for particular countries, as the EU did for the U.S. under the former Safe Harbor agreement mentioned above, may violate the obligation on all WTO Members to accord most-favored-nation (MFN) treatment under GATS art II:1.[84] Those obligations are subject to Members' listed exemptions under GATS art II:2. In the absence of a relevant exemption, relaxing or excluding particular countries (or suppliers from particular countries) from data transfer restrictions is likely to constitute more favorable treatment contrary to GATS art II:1. The member providing such preferential treatment would then need to justify that treatment, either under a general exception or a national security exception of the kind discussed below, or under the exception in GATS art V for economic integration agreements.

3 Domestic Regulation (GATS Art VI): Burdensome Privacy-Based Requirements

GATS also imposes general, non-contingent obligations on all Members in relation to domestic regulation under art VI. Under GATS art VI:1, in those service sectors in which a Member has made specific commitments (that is, market access, national treatment, or additional commitments), the Member must "ensure that all measures of general application affecting trade in services are administered in a reasonable,

---

82 *See* Appellate Body Report, *China – Publications and Audiovisual Products*, *supra* note 37, at ¶¶ 412-13.

83 Panel Report, *China – Electronic Payment Services*, *supra* note 74, ¶¶7.204, 8.1(b)(i).

84 Reyes, *supra* note __, at 153-57.

objective and impartial manner."[85] For those same sectors, under GATS art VI:5(a)(i) (through its reference to GATS art VI:4), Members must ensure that "licensing and qualification requirements and technical standards" do not "nullify or impair" its commitments, for example through the absence of "objective and transparent criteria" or being "more burdensome than necessary to ensure the quality of the service."[86]

It has been argued that "the present interpretation of Article VI . . . does not leave a wide discretion for national legislators to introduce high privacy standards (for example on sensitive data or registration of data collection)."[87] Registration and authorization requirements for data collection can considerably increase costs of compliance for foreign service suppliers. For example, requirements to obtain consent before transmitting personal information across borders may be complicated when information involving a range of actors is relevant to a particular application or device.[88] The likelihood of violation will depend on the specific measure and the surrounding circumstances.

4 Market Access (GATS Art XVI): The Problem of Zero Quotas

GATS art XVI sets out the market access obligations that apply according to the commitments made by a Member in its GATS schedule regarding the relevant mode and service sector. Unless relevant limitations or conditions are included in the schedule, a Member that has made a market access commitment to a given sector must not limit "the number of service suppliers" (art XVI:2(a)) or "the total number of service operations or … the total quantity of service output" (art XVI:2(c)). Significantly for data transfer restrictions, the Appellate Body found in *U.S. — Gambling* that a "prohibition on the remote supply of gambling and betting services" online is effectively a "zero quota" in breach of GATS arts XVI:2(a) and (c).[89]

Similar reasoning could apply to any restriction on cross-border transfer of entire categories of data, for whatever reason, to the extent that these categories correspond to service

---

85 GATS art. VI, ¶5(a).

86 GATS art. VI, ¶ (4).

87 Rolf Weber, *Regulatory Autonomy and the Privacy Standards under the GATS,* 7 ASIAN J. WTO & INT'L HEALTH L. &POL'Y 25, 37 (2012).

88 Usman Ahmed & Anupam Chander, *Information Goes Global: Protecting Privacy, Security, and the New Economy in a World of Cross-border Data Flows* 6-7 (E15 Expert Group on the Digital Economy, Think Piece, International Centre for Trade and Sustainable Development and World Economic Forum, Nov. 2015).

89 Appellate Body Report, *supra* note __, at ¶ 373(C)(i), 238, 251.

sectors or sub-sectors in which the relevant Member has made market access commitments without relevant qualifications. Thus, measures such as the EU Privacy Directive (discussed above) could violate both the domestic regulation obligations in GATS art VI and the market access obligations in GATS art XVI. [90] In addition to those provisions, a WTO Member imposing high privacy standards regarding cross-border delivery of electronic services could violate its national treatment commitments in the relevant sector under GATS art XVII.[91]

5 General Exceptions (GATS Art XIV): Central to WTO-Consistency

Even if a substantive violation of GATS might arise, the effect of the exceptions clauses in GATS must also be considered. Firstly, the general exceptions clause in GATS art XIV is modeled on GATT art XX, such that the WTO case law on each provision refers to that on the other, with parallel tests applying under both. GATS art XIV provides an (apparently exhaustive) list of 'general exceptions' from GATS obligations in the following terms:

> Subject to the requirement that such 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, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures:
>
> (a) necessary to protect public morals or to maintain public order; . . .
>
> (c) necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to:
>
> (i) the prevention of deceptive and fraudulent practices or to deal with the effects of a default on services contracts;
> (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and

90 Reyes, *supra* note __, at 153-57.
91 Weber, *supra* note __, at 32.

> the protection of confidentiality of individual records and accounts;
> (iii) safety; . . . [92]

While the other paragraphs under GATS art XIV are less relevant, paragraphs (a) and (c) may encompass certain cross-border data transfer restrictions. In examining a challenged measure under GATS art XIV, a WTO panel or the Appellate Body would first identify the objective of the measure (taking account of not just the respondent's declaration of the objective, but also other evidence such as the legislative history, structure, and operation of the measure)[93] and then determine whether that objective falls within the general scope of the relevant paragraph.

As regards paragraph (a), a data transfer restriction could have a legitimate objective of protecting public morals. Public morals in this context "denotes standards of right and wrong conduct maintained by or on behalf of a community or nation," [94] and WTO tribunals have given considerable deference to governments in identifying their public morals and the measures to be taken for public morals purposes.[95] Difficult questions could arise concerning measures that appear to be designed to restrict free expression or to repress political dissent, perhaps contrary to norms of public international law, including human rights law.[96] However, the WTO might not need to deal with such questions directly, since the respondent government is likely to put forward a legitimate objective such as protecting public morals even if that is not the true objective. GATS art XIV has a complex and demanding test for compliance (as explained further below), which is likely to reveal any use of "public morals" as a cover for protectionist measures or for other objectives not recognized as legitimate in GATS art XIV.

As regards paragraph (c), WTO Members have previously faced difficulties in establishing that their challenged measures were intended to "secure compliance" with WTO-consistent domestic laws. Securing compliance with an international law as such (rather than as implemented into domestic law) would not bring a measure within the scope of

---

92 GATS art. XIV.

93 *See* Appellate Body Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products*, ¶ 5.144, WT/DS400/AB/R (May 22, 2014) [hereinafter *EC – Seal Products*].

94 *China – Publications and Audiovisual Equipment*, ¶ 7.759 (quoting Panel Report, *supra* note __, at ¶ 6.465)

95 *See, e.g.*, U.S. – Gambling at ¶ 299; China – Publications and Audiovisual Products at ¶ 7.766]; EC – Seal Products at ¶ 5.167.

96 SARAH JOSEPH, BLAME IT ON THE WTO? A HUMAN RIGHTS CRITIQUE 139 (2011).

paragraph (c).[97] A domestic law that was inconsistent with WTO law would also not meet the terms of paragraph (c). Thus, although paragraph (c)(ii) refers explicitly to privacy, confidentiality, and personal data, it would not necessarily be an easier justification to make out than paragraph (a).

After identifying a measure falling within the general scope of paragraph (a) and/or (c), a respondent Member would also need to satisfy a "necessity" test, demonstrating that the measures are "necessary to" achieve the stated objective. That test "involves a process of 'weighing and balancing' a series of factors, including the importance of the objective, the contribution of the measure to that objective, and the trade-restrictiveness of the measure."[98] Most objectives are likely to be accepted as important, particularly public morals and privacy since they are explicitly recognized in the treaty text.[99] The more difficult questions are likely to surround the measure's contribution to its objective and its trade-restrictiveness. The more a measure contributes to its objective, the more trade-restrictiveness is likely to be tolerated. Conversely, the more trade-restrictive a measure (with an import ban being the archetype of the most trade-restrictive measure possible, arguably corresponding to a complete ban on cross-border transfer of particular categories of data), the greater the contribution to the objective that the respondent Member will have to demonstrate.

A requirement to store data locally may restrict trade due to the difficulty faced by foreign firms in complying with the requirement in a cost-effective manner. Unless locally based, they are likely to be at a disadvantage when compared to local firms. Multinational companies with models based on centralization may also face somewhat higher costs in complying with such jurisdiction-specific localization requirements. At the same time, the contribution of such a requirement to the goal of privacy or national security may be compromised to the extent that it can be shown that server localization actually compromises the security of data, by

---

97 See Appellate Body Report, *Mexico – Tax Measures on Soft Drinks and Other Beverages*, ¶ 79, WT/DS308/AB/R (Mar. 6, 2006).

98 *EC – Seal Products* at ¶ 5.169 (citing Appellate Body Report, *Korea – Measures Affecting Imports of Fresh, Chilled and Frozen Beef* ¶ 164, WT/DS161/AB/R (Dec. 11, 2000); Appellate Body Report, *United States — Gambling, supra* note 37, at ¶ 306; Appellate Body Report, *Brazil – Measures Affecting Imports of Retreaded Tyres*, ¶ 182, WT/DS332/AB/R (Dec. 3, 2007). *See also China – Publications and Audiovisual Products*, *supra* note 37, ¶¶ 239-42.

99 WTO tribunals have recognised a number of objectives as important (*see, e.g.*, Appellate Body Report, *European Communities – Measures Affecting Asbestos and Asbestos-Containing Products*, ¶ 172, WT/DS125/AB/R (Mar. 12, 2001)) and would not generally declare that a particular government objective is unimportant.

preventing "sharding" [100] and increasing susceptibility to malware and other attacks. These kinds of measures may therefore face problems in establishing necessity under GATS art XIV(a) or (c), depending on the specific circumstances and available evidence.

If the challenged data transfer restriction nevertheless satisfied the weighing and balancing test, a WTO panel or the Appellate Body would have to consider—as a final element of the necessity test—whether a less trade-restrictive alternative existed that was reasonably available to the respondent Member and that would make an equal contribution to the identified objective.[101] Several alternatives to data localization may be possible, such as end-to-end encryption technologies.[102] Alternatives to banning cross-border data transfer for privacy purposes could include employing consent mechanisms for use of data or remedial measures such as providing individual access to data to enable corrections. Fewer alternatives may exist, however, to banning data transfer on national security or public morals grounds, since it is the content of the data itself that raises the perceived problem for states.[103] The availability of such measures to a respondent Member would depend on technical feasibility as well as the Member's financial and professional resources. The outcome would again depend on the particular nature and framing of the measure and the factual circumstances.

If the challenged data transfer restriction was found provisionally necessary under paragraph (a) or (c) of GATS art XIV, the final question would be whether it meets the stringent requirements of the chapeau of GATS art XIV. The Appellate

---

100 Data sharding "breaks off part of the data in a horizontal partition, providing enough data to work with but not enough to reidentify an individual.". David Geer, *Big Data Security, Privacy Concerns Remain Unanswered*, CSO (Dec. 5 2013), http://www.csoonline.com/article/2134203/mobile-security/big-data-security--privacy-concerns-remain-unanswered.html.

101 Appellate Body Report, *Korea — Measures Affecting Imports of Fresh, Chilled and Frozen Beef*, ¶ 166, WTO Doc. WT/DS161/AB/R (Dec. 11, 2000) [herafter *Korea—Beef*].

102 End-to-end encryption technologies enable data to be transferred uninterrupted by the underlying communication networks (such as telecom service providers or internet service providers) such that only the end recipient can decrypt the data, thus ensuring the integrity of the data through the process of transfer. Andy Greenberg, *Hacker Lexicon: What is End-to-End Encryption?*, WIRED (Nov. 25, 2014), . https://www.wired.com/2014/11/hacker-lexicon-end-to-end-encryption/.

103 More selective filtering may, however, assist a state to defend its blocking measures. *See* Brian Hindley & Hosuk Lee-Makiyama, *Protectionism Online: Internet Censorship and International Trade Law*,6 (ECIPE Working Paper 12/2009), ecipe.org/publications/protectionism-online-internet-censorship-and-international-trade-law; Claude Barfield, *China's Internet Censorship: A WTO Challenge is Long Overdue*, AMERICAN ENTERPRISE INSTITUTE (Apr. 29, 2016), www.aei.org/publication/chinas-internet-censorship-a-wto-challenge-is-long-overdue/.

Body has highlighted the use of the word "applied" in the chapeau,[104] suggesting that it would consider how a data transfer restriction is implemented and operates in practice. Any apparent arbitrariness or discrimination in the application of the restriction—for example, if exceptions to security or privacy standards imposed on data transfer are made for particular countries, or if established standards are not applied consistently to each country from day to day—is likely to create problems for its justification under the chapeau. The treatment of domestic data transfer could also demonstrate discrimination or arbitrariness, for example if local services or suppliers are exempt from prohibitions on certain kinds of online content.

6 National Security Exceptions (GATS Art XIVbis): Limited Relevance

GATS art XIV*bis* preserves WTO Members' regulatory autonomy in relation to national security, but it is limited to particular circumstances. In particular, GATS art XIV *bis*:1(b) provides that nothing in GATS is to be construed

> to prevent any Member from taking any action which it considers necessary for the protection of its essential security interests:
> (i) relating to the supply of services as carried out directly or indirectly for the purpose of provisioning a military establishment;
> (ii) relating to fissionable and fusionable materials or the materials from which they are derived;
> (iii) taken in time of war or other emergency in international relations; or . . .[105]

Although this provision may be seen as "self-judging" because of the words "action which it considers necessary," the inclusion of the sub-paragraphs (i) to (iii) significantly limits its relevance to particular scenarios. Article XIV*bis*:1(b)(i) is likely to cover data transfer restrictions in relation to digital services provided in connection with military establishments, while art XIV*bis*:1(b)(ii) would cover transfer restrictions related specifically to data concerning fissionable and fusionable materials. Article XIV*bis*:1(b)(iii) is more broadly worded and could potentially justify a very wide range of cross-border data transfer restrictions taken in time of war (which could perhaps include civil uprising or cyberwarfare, to the extent that the

---

[104] Appellate Body Report, *United States – Standards for Reformulated and Conventional Gasoline*, ¶ 22, WTO Doc. WT/DS2/AB/R (29 April 1996).

[105] GATS art. XIV *bis*, ¶1(b).

term "war" is inherently "evolutionary") [106] or other international emergency. Some leeway exists for a WTO Member to interpret such circumstances broadly, but they would not seem to cover blanket restrictions on particular types of data transfer operating on a routine rather than exceptional basis.

These exceptions may be relevant to measures such as the U.S. recommendation to telecommunications firms not to purchase Huawei equipment, Australia's ban on such equipment in its National Broadband Network due to concerns of cyber espionage, or China's ban on several U.S. services, like Microsoft Windows, in governmental agencies. [107] (Although these measures are not *per se* restrictions on cross-border data transfer, they nevertheless relate to cross-border data transfer, illustrating the kinds of rationales and actions that a government might adopt.) One author has proposed a principle of good faith to assess whether a particular measure is genuinely considered necessary for essential security interests.[108] Whether such a defense would be made out, in the absence of a war or emergency, remains to be seen. WTO Members may be reluctant to raise such matters in WTO disputes for fear of further jurisprudential interventions on the meaning of the national security exceptions.[109]

7 Conclusion

Considerable uncertainty arises in applying WTO law to Members' restrictions on cross-border data transfer, from the initial questions of classifying the relevant products as goods or services or within services, to the application of core GATS obligations. The uncertainty and lack of specificity in WTO rules in this area likely means that particular measures will have to be assessed when a dispute arises, with much depending on the interpretation and application of the exceptions in GATS art XIV. In the absence of more specific rules, arising from a failure to achieve consensus on how to deal with these modern technologies and practices, Members will have to accept and abide by the recommendations and

---

106 *Cf* .Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 130, WTO Doc. WT/DS58/AB/R (Oct. 12, 1998).

107 Shin Yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 J. OF INT'L ECON. L. 449, 450, 453 (2015).

108 *Id.* at 466-68.

109 WTO members have shown a similar reluctance to challenge measures purportedly justified by other exceptions, such as the exception for regional economic integration agreements in GATS art V and its equivalent in GATT art XXIV.

rulings of WTO Panels and the Appellate Body, as adopted by the WTO Dispute Settlement Body.

B Remaining Gaps in TPP Provisions on Cross-Border Data Transfer

1 Scope of Chapter 14 and Underlying Rationale

Due to the slow progress of negotiations on e-commerce and digital issues within the multilateral framework of the WTO, mega-regionals such as the TPP have become important platforms to regulate restrictions on cross-border data transfer. The TPP has introduced, for the first time, binding provisions prohibiting data localization and imposing requirements on cross-border transfer of data in the Electronic Commerce chapter (Chapter 14) of the TPP.[110] If the TPP enters into force, it will be the first trade or investment agreement to prohibit interference with cross-border transfer of information by electronic means.[111] Prior to the TPP, the *Free Trade Agreement between the United States of America and the Republic of Korea* (KORUS FTA)[112] required the parties only to "endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."[113]

The policy rationale behind TPP ch 14 is to facilitate an open Internet and the free flow of e-commerce across borders.[114] Article 14.2.1 confirms this rationale:

> The Parties recognise economic growth and opportunities provided by electronic commerce and

---

110 Certain exemptions were made: it was agreed that Australia would not be required to change the stated restrictions on cross-border transfers of e-health records of its citizens under domestic law, and Vietnam and Malaysia were given an additional 2 years to comply with the provisions, during which no legal action could be brought against them, under the dispute settlement process. Vietnam also secured a 2-year extension in order to align their server localization policies with the TPP provision to do away with localization of computing facilities.

111 Department of Foreign Affairs and Trade, 'Trans-Pacific Partnership Agreement: an Introduction by the Department of Foreign Affairs and Trade'. But see the PTA between the United States and Korea, art 15.8.

112 Consolidated KORUS FTA Text (signed on 30 June 2007, entered into force 15 March 2012) <https://ustr.gov/trade-agreements/free-trade-agreements/korus-fta/final-text>.

113 KORUS FTA art 15.8. See also KORUS annex 13-B, section B, which states: 'Each Party shall allow a financial institution of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the institution's ordinary course of business.'

114 Drennan et al, *Privacy Law, Cross-Border data Flows and the Trans-Pacific Partnership Agreement*, *supra* note 61.

> the importance of frameworks that promote consumer confidence in electronic commerce and of avoiding unnecessary barriers to its use and development.

Chapter 14 applies "to measures adopted or maintained by a Party that affect trade by electronic means,"[115] but not to government procurement[116] or to "information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection."[117] Thus, the chapter is focused on commercial transactions, rather than government processing of information. Measures requiring local storage of government data will be unaffected, even where commercial entities are engaged by or on behalf of the government to store the data.

Chapter 14 imposes a number of obligations and sets out additional aspirational principles concerning electronic commerce. For example, art 14.3.1 precludes a TPP party from imposing customs duties on electronic transmissions between a person of one party and a person of another party. In the WTO, a moratorium continues to apply on customs duties in such circumstances, in the absence of longer-term agreement on the matter.[118] Article 14.4.1 precludes parties from according "less favorable treatment" to digital products of other TPP parties or their citizens than "to other like digital products" (which would include those of the first party and TPP non-parties),[119] thus encompassing both the national treatment and MFN treatment limbs of WTO non-discrimination.

We now turn to the most important provisions of ch 14 for cross-border data transfer: art 14.11, which requires parties to allow cross-border data transfer, and art 14.13, which prohibits parties from requiring computing facilities to be locally based.

2 Parties Shall Allow Cross-Border Data Transfer (TPP Art 14.11)

Article 14.11.2 of the TPP provides:

> Each Party shall allow the cross-border transfer of information by electronic means, including personal

---

115 TPP art 14.2.2.

116 TPP art 14.2.2.

117 TPP art 14.3(b).

118 WTO Ministerial Conference, *Work Programme on Electronic Commerce, Adopted on 19 December 2015,* ¶ 3, WTO Doc. WT/MIN(15)/42 WT/L/977 (Dec. 21, 2015).

119 TPP art 14.4.1, n. 4.

> information, when this activity is for the conduct of the business of a covered person.

A "covered person" is exhaustively defined in art 14.1 to mean a covered investment or an investor of a party, as defined in ch 9 (Investment), or a service supplier of a party, as defined in ch 10 (Services). Financial institutions are excluded, as discussed further below.

The obligation in art 14.11.2 is qualified by an exception that reflects in part GATT art XX/GATS art XIV, such that TPP parties may adopt measures inconsistent with art 14.11.2 "to achieve a legitimate public policy objective," provided that the measure:

> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable discrimination or a disguised restriction on trade; and
> (b) does not impose restrictions on transfers of information greater than are required to achieve the objective.

The term "legitimate public policy objective" is not defined, creating ambiguity, particularly as the TPP parties may not share the same values regarding data protection and related questions. In a dispute under the state-state dispute resolution provisions in Chapter 28, a treaty interpreter might turn to the objectives of Chapter 14—and of the TPP as a whole—and also to TPP art 29.3 for context.[120] That provision incorporates GATS art XIV(a), (b), and (c) into the TPP, *mutatis mutandis*, for the purpose of Chapter 14 (among others). Therefore, the references in GATS art XIV to concepts such as public morals, public order, privacy, and consumer protection may suggest that these are legitimate public policy objectives for the purpose of art 14.11.2.

The terms of art 14.11.2(a), which reflect those of the chapeau of GATT art XX (and less directly GATS art XIV), may lead the interpreter to refer to WTO jurisprudence on these provisions as informative or as providing relevant guidance[121]—a tendency that may be likely across the TPP

---

[120] There is a separate international treaty, the Vienna Convention on the Law of Treaties, that governs treaty interpretation issues such as how to interpret ambiguous terms. *See* Vienna Convention on the Law of Treaties, art 31(1), May 23, 1969, 1155 U.N.T.S. 331 (entered into force Jan. 27, 1980) [hereinafter VCLT].

[121] For example, as evidence indicating the 'ordinary meaning' of the terms under VCLT art 31(1), as 'relevant rules of international law applicable in the relations between the parties' under VCLT art 31(3)(c) (to the extent that rulings adopted by the WTO Dispute Settlement Body may be seen as a

treaty, given the well-established WTO case law relating to WTO provisions on which many of the TPP provisions are based. The reference in TPP art 14.11.2(b) to restrictions that are greater than required to achieve the objective might similarly create a tendency to refer to WTO case law, for example on GATS art IV:5(a)(i) or art 2.2 of the *Agreement on Technical Barriers to Trade*.[122] However, even in the WTO, as seen from the discussion of the general exceptions above, many concepts remain elusive, including such common touchstones as trade-restrictiveness.[123] Just as in the WTO, leaving too much to be determined in a dispute by the meaning of the term "legitimate public policy objective" may undermine the specific nature of these data transfer provisions in the TPP. This problem is exacerbated in both the WTO and TPP contexts by the often-technical nature of data transfer and data security, which is likely to fall beyond the expertise of trade tribunals.

3 Parties Shall Not Require Local Computing Facilities (TPP Art 14.13)

Article 14.13.2 of the TPP states that prohibits localization requirements as follows:

> 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.[124]

However, like the primary obligation in art 14.11.2, the prohibition in art 14.13.2 is subject to a qualification in art 14.13.2 (very similar to art 14.11.3):

> Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with paragraph 2 to achieve a legitimate public policy objective, provided that the measure:
> (a) is not applied in a manner which would constitute a means of arbitrary or unjustifiable

---

subsidiary means of establishing law under *ICJ Statute* art 38(1)(d), or simply as supplementary means of interpretation under VCLT art 32.

122 *Marrakesh Agreement Establishing the World Trade Organization*, opened for signature Apr. 15, 1994, 1868 U.N.T.S. 3 (entered into force Jan. 1, 1995), annex 1A [hereinafter *Agreement on Technical Barriers to Trade*].

123 *See generally* Tania Voon, *Exploring the Meaning of Trade-Restrictiveness in the WTO*, 14 WORLD TRADE REV. 451 (2015).

124 Computing facilities are defined in the TPP as 'computer servers and storage devices for processing or storing information for commercial use.' *See* TPP art 14.1. This definition incorporates cloud computing services.

discrimination or a disguised restriction on trade; and

(b) does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective.

This broad exception suffers from the same difficulties as those described above in relation to art 14.11.3, again limiting its ability to facilitate cross-border data flows.

4 Exclusion of Financial Institutions from TPP Arts 14.11 and 14.13

The TPP requirements to allow cross-border data transfer (art 14.11.2) and not to require local computing facilities as a condition for conducting business (art 14.13.2) are phrased with respect to "a covered person," making the definition of covered person significant. Article 14.1 defines a covered person as excluding a "financial institution," a "cross-border financial service supplier of a party," and "an investor in a financial institution." Thus, the data transfer and localization provisions of TPP ch 14 do not generally apply to financial services and institutions. Nevertheless, the TPP contains a separate data transfer requirement for the financial sector: "Each Party shall allow a financial institution of another Party to transfer information in electronic or other form, into and out of its territory, for data processing if such processing is required in the institution's ordinary course of business."[125] (That provision goes on to confirm that TPP parties may in certain circumstances restrict data transfer in order to protect personal data, personal privacy or confidentiality of individual records or accounts, or for prudential reasons.) The exclusion of the financial sector from the more stringent localization and data transfer requirements in the general Electronic Commerce chapter has created some concern, leading to proposed changes in other agreements as discussed further below.

5 Legal Framework for Protecting Personal Information (TPP Art 14.8)

Article 14.8.1 of the TPP recognizes "the economic and social benefits of protection the personal information of users of electronic commerce and the contribution that this makes to enhancing consumer confidence in electronic commerce." Accordingly, under art 14.8.2, each TPP party "shall adopt or maintain a legal framework that provides for the protection of

[125] *See* s B of annex 11B to the TPP ch 11 (Financial Services).

the personal information" of those users. This obligation to construct a legal framework may be seen as a way of alleviating concerns about enhancing the free flow of data among TPP parties. Rather than adopting data transfer restrictions or data localization requirements in order to prevent privacy breaches, parties allow data to flow to other TPP countries subject to obligations on those countries to protect that data. (Several other provisions can be seen in the same light, such as the requirement to adopt consumer protection laws in art 14.7.) In addition, art 14.8.3 requires each party to "endeavor to adopt non-discriminatory practices in protecting" e-commerce users from "personal information protection violations." Article 14.8.4 states that each party "should publish information" on how e-commerce users can pursue remedies and how "business" can comply with "any legal requirements."

Among the TPP parties, significant regulatory diversity exists in relation to privacy and data protection. Canada, New Zealand, and Australia have evolved privacy regimes; the U.S. has an *ad hoc* regime with a mixture of sector-specific regulations and self-regulatory codes; Vietnam has recently implemented a law to protect personal information online;[126] Brunei Darussalam, meanwhile, does not yet have a privacy law in place.[127] Thus, under note 5 to art 14.8, Brunei Darussalam and Vietnam are not required to apply art 14.8 before they have implemented the relevant legal framework—a rather circular note, suggesting that no deadline applies for those parties. This exception may undermine the value of the requirement to adopt a legal framework and other protections under art 14.8, since the very countries that are lacking those protections are the ones not obliged to impose them.

Article 14.8.5 recognizes that TPP parties "may take different legal approaches to protecting personal information." It therefore states that parties should "encourage the development of mechanisms to promote compatibility" between their different approaches to protecting personal information, such as through autonomous or mutual recognition arrangements or through 'broader international frameworks." Similarly, in developing the legal framework, art 14.8.2 specifies that parties "should take into account principles and guidelines of relevant international bodies."[128] However, no

---

126 Law on Network Information Security, 2015, Law no.: 86/2015/QH13, arts. 16-20, http://english.mic.gov.vn/Upload/VanBan/Law-on-Network-Information-Security-16-05-30.pdf.

127 *See* NORTON ROSE FULBRIGHT, BUSINESS ETHICS AND ANTI-CORRUPTION LAWS: BRUNEI DARUSSALAM 5 (2014), http://www.nortonrosefulbright.com/knowledge/publications/121089/business-ethics-and-anti-corruption-laws-brunei-darussalam#section14?.

128 TPP art 14.8.2.

well-established international privacy standards have been developed; nor does the TPP text specify any further benchmarks for assessing legal frameworks developed by TPP parties under art 14.8.2.

Some high-level principles have been adopted in bodies such as the Asia-Pacific Economic Co-operation (APEC)[129] and the Organization for Economic Co-operation and Development (OECD).[130] The *APEC Privacy Framework* "is intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted."[131] This framework is not legally binding, recognizes self-regulatory standards as a form of privacy protection,[132] and is based on broad principles including preventing misuse of personal information,[133] providing notice to users regarding collection and use of data,[134] accountability of data controllers,[135] and maintaining integrity of personal data.[136] The *OECD Privacy Framework*, while based on similar principles, contains stronger implementation guidelines for member countries including development of national privacy strategy alongside adoption of privacy laws and enforcement mechanisms,[137] and providing notifications pertaining to data breaches.[138] Although the *APEC Privacy Framework* is supported by the US[139] and appears aligned with TPP art 14.8.2, its effectiveness remains debated.[140] Evidently, further discussion of these kinds of standards and principles is needed at the international level, not just in connection with the TPP or the WTO, or trade and investment law in general, but more broadly.

---

129 Asia Pacific Economic Cooperation, APEC Privacy Framework, APEC#205-SO-01.2 (2005), http://www.apec.org/Groups/Committee-on-Trade-and-Investment/~/media/Files/Groups/ECSG/05_ecsg_privacyframewk.ashx [hereinafter APEC Privacy Framework].

130 Organisation for Economic Co-operation and Development, The OECD Privacy Framework (2013) http://www.oecd.org/sti/ieconomy/oecd_privacy_framework.pdf [hereinafter OECD Privacy Framework].

131 APEC Privacy Framework, 4.

132 *Id*. at 11.

133 *Id*.

134 *Id*. at 12.

135 *Id*.

136 *Id*. at 20.

137 OECD Privacy Framework, 17.

138 *Id*. at 16.

139 *U.S. Examining How APEC Work Could Inform TPP Negotiations*, WORLD TRADE ONLINE (Mar. 5, 2010), https://insidetrade.com/inside-us-trade/us-examining-how-apec-work-could-inform-tpp-negotiations. *U.S.*

140 *See, e.g.*, Joshua P. Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2 ASIA & THE PAC. POL'Y *Studies* 90, 93-94 (2014); *cf* Graham Greenleaf, *Five years of the APEC Privacy Framework: Failure or Promise?*, 25 COMPUTER L. & SECURITY REV. 28, 29-33 (2009).

6 Conclusion

The TPP introduces welcome specificity into the international trade law field, providing clearer obligations and principles in relation to data transfer than have previously existed in the WTO or elsewhere. However, the inability of even the 12 TPP parties to agree on precise requirements means that several areas remain unaffected or subject again to the discretion of those deciding TPP disputes, just as in the WTO context discussed above. In particular, financial services are excluded from the application of the two core data transfer provisions (arts 14.11.2 and 14.13.2), those core provisions are subject to significant questions about the meaning of a "legitimate public policy objective" and the means justified to achieve such an objective, and two parties are effectively exempt from the requirement to establish a legal framework for the protection of personal information. The TPP confirms the difficulty in making progress on these issues in a plurilateral or multilateral setting, while implicitly highlighting areas that will need further work if trade and investment law is to better support the digital economy.

C Developments in TTIP and TiSA: EU Position Precludes Data Flow Provisions

After the TPP negotiations were concluded in October 2015, the possibility of establishing a side agreement relating specifically to the financial services industry was brought up by a bipartisan group of U.S. lawmakers,[141] to address the problem of the exclusion from key data transfer and localization provisions in the TPP text. The U.S. Treasury Secretary Jack Lew referred to the difficult balance required: preventing data localization requirements from being used as non-tariff barriers, while making sure prudential regulators have access data when necessary.[142] He adopted a cautious approach to a side agreement, instead emphasizing the importance of these discussions in informing future

---

141 Alex Lawson, *Polls Call For New TPP Data Rules For Banking Sector*, LAW 360 (Jan. 12, 2016), https://www.law360.com/articles/745615/pols-call-for-new-tpp-data-rules-for-banking-sector. *See also* Nigel Cory and Robert D Atkinson, *Financial Data Does Not Need or Deserve Special Treatment in Trade Agreements*, INFORMATION TECHNOLOGY AND INNOVATION FOUNDATION (April 2016), http://www2.itif.org/2016-financial-data-trade-deals.pdf?_ga=1.224805651.860038149.1486093734 (arguing that an exemption for financial services data flows creates a policy loophole that could be exploited by other nations).

142 *See Lew Floats Possibility of Side Deal to Address TPP Data Localization*, WORLD TRADE ONLINE (Mar. 16, 2016), https://insidetrade.com/daily-news/lew-floats-possibility-side-deal-address-tpp-data-localization.

negotiations.[143] The U.S. Treasury, a group of U.S. finance companies and U.S. lawmakers have since developed a proposal to prohibit data localization requirements in the financial services industry in ongoing and future trade negotiations, to be enforceable through a state-to-state dispute settlement mechanism.[144] The USTR has clarified that the data localization issue for financial services will be resolved in the TiSA and TTIP negotiations. For TPP parties not participating in TiSA, the U.S. government will determine individual arrangements to ensure that data localization restrictions are not imposed in the financial services sector.[145] These kinds of changes would enhance the possibility of further liberalization of financial services.

Although the TPP has set some limited standards regarding cross-border data transfer, it may not be easy for the U.S. to negotiate for similar provisions in trade negotiations with the EU such as the TTIP and TiSA. In light of the ECJ judgment in *Schrems v Data Protection Commissioner*, some European Commission officials have taken the view that in order to remain compliant with the data protection laws within EU, the best policy option for technology companies is to store the personal data of EU citizens within its borders.[146] In spite of strong pressure from the U.S., in the TiSA negotiations, the EU has exhibited reluctance to change its position regarding data localization and cross-border information flows.[147] The May 2016 leaked draft of the TiSA also shows that the EU has not offered any commitments regarding cross-border information flows or prohibition of localization provisions, or other related rules related to privacy, and transfer or access to

---

143 *Lew Reiterates Possibility of TPP Side Deal, But Emphasizes Future Fix*, WORLD TRADE ONLINE (Mar. 23, 2016), https://insidetrade.com/daily-news/lew-reiterates-possibility-tpp-side-deal-emphasizes-future-fix.

144 Len Bracken, *Treasury Financial Services Industry Agree on Data Proposal*, BLOOMBERG BNA (May 25, 2016), https://www.bna.com/treasury-financial-services-n57982073068/.

145 *Data Fix Prompts Major Financial Services, Insurance Associations to Back TPP*, WORLD TRADE ONLINE (July 14, 2016), https://insidetrade.com/inside-us-trade/data-fix-prompts-major-financial-services-insurance-associations-back-tpp. *U.S.*

146 *See* Press Release, The Hamburg Commissioner for Data Protection and Freedom of Information, Administrative Order Against the Mass Synchronisation of Data Between Facebook and WhatsApp (Sep. 27, 2016), https://www.datenschutz-hamburg.de/fileadmin/user_upload/documents/Press_Release_2016-09-27_Adminstrative_Order_Facebook_WhatsApp.pdf; *cf. Privacy Law, Cross-Border Data Flows, and the Trans Pacific Partnership Agreement: What Counsel Need to Know*, KING AND SPALDING LLP (Nov. 10, 2015) http://www.kslaw.com/imageserver/KSPublic/library/publication/ca111015.pdf.

147 BRYCE BASCHUK, LATEST EU OFFER NOT NEGOTIABLE: TISA NEGOTIATORS SAY (May 27, 2016) Bloomberg BNA WTO Reporter.

source code in the Electronic Commerce chapter.[148] The EU also holds a similar negotiating position in the TTIP negotiations, including a rejection of the prohibition on data localization in financial services.[149] Given that the EU is the top exporter of digitally deliverable services,[150] its negotiating position may have a strong impact on how data transfer provisions are executed in future trade agreements. The apparent ideological divide in this area between the EU and the U.S. does not bode well for future progress.

IV DATA FLOWS UNDER INTERNATIONAL INVESTMENT LAW

Alongside trade law, the international investment law regime is likely to play a key role in regulating state restrictions on cross-border transfer of data. States may be motivated to impose such restrictions by the same rationales as discussed above, namely national security, public morals or privacy. In the following sections, we show that a potential claimant affected by state restrictions on data transfer would likely be able to meet the preliminary hurdles of proving that it holds an investment, in the territory of the host state, in order to seek investment treaty protection.[151] It is less clear, though, that any violation of an investment treaty guarantee would be made out. The outcome is likely to be highly fact-dependent, with a claim for fair and equitable treatment, for instance, being more prone to succeed if the claimant can demonstrate that restrictions on data transfer were passed for political motives or at short notice. If a violation is found, however, states are unlikely to be able to defend their conduct by reference to an exceptions clause in an investment treaty. Such clauses, even where they exist, largely do not contain exceptions relevant in the data transfer context, and are in any case generally accepted to establish high thresholds. Lastly, while more recent prominent trade and investment agreements (such as the TPP) have included specific provisions on data transfer, these are not likely to assist greatly in investment treaty arbitration proceedings.

---

148 *See* Trade in Services Agreement (TiSA) Annex on Electronic Commerce, art 2 (2013), https://wikileaks.org/tisa/document/20151001_Annex-on-Electronic-Commerce/20151001_Annex-on-Electronic-Commerce.pdf.

149 MICHAEL SCATURRO, EU TO PUSH FOR ITS DATA PROTECTION IN TRADE DEALS (May 26, 2016) Bloomberg BNA International Trade Daily.

150 In 2016, U.S. exports of digital services were valued at USD $380 billion, while EU exports were valued at USD $465 billion. *See Id.* U.S.

151 The claim must of course pass other jurisdictional hurdles not discussed here, such as the existence of a bilateral investment treaty in force between the home and host states.

A Threshold Requirements: Complicated But Likely Met

1 Existence of an 'Investment' under the ICSID Convention and the IIA

Any party wishing to bring a claim against a host state under an investment treaty must fulfill the gateway requirement that they hold an "investment," as defined by the relevant international investment agreement (IIA) and, if claiming under the auspices of the *Convention on the Settlement of Investment Disputes between States and Nationals of Other States* (ICSID Convention),[152] as understood in that Convention as well. It has proven difficult to classify the legal nature of data in many contexts.[153] As noted above, uncertainty remains in WTO law as to the proper classification of data. It is also potentially unclear whether data counts as property, and, if so, whether it is personal property or intellectual property. However, many of these conceptual difficulties are likely to be sidelined in the field of international investment law. The protection of an investment treaty is predicated on the existence of an "investment," a concept broader than "property." An investment treaty claimant would most likely not claim that particular data, the transfer of which may have been restricted or interfered with, itself constituted the investment to activate a treaty's protection. Instead, the claimant would emphasize that tribunals have typically seen investment as a holistic process, covering a range of activities over time, potentially in different locations, and in a variety of tangible and intangible forms.[154] Indeed, standard treaty definitions of investment are inclusive and very broad, frequently phrased as covering "all assets."[155]

Under the ICSID Convention, investment is often taken to be a slightly more substantive concept, calling for some kind of contribution from the investor and a sufficient level of risk and duration.[156] It is difficult to assess these three so-called

---

152 Convention on the Settlement of Investment Disputes between States and Nationals of Other States, Mar. 18, 1965, 4 I.L.M. 524 (1965), art 63 [hereinafter ICSID Convention].

153 For some difficulties in another area of international law, see Kubo Mačák, *Military Objectives 2.0: The Case for Interpreting Computer Data as Objects under International Humanitarian Law*, 48 *Israel Law Review* 55 (2015).

154 RUDOLF DOLZER & CHRISTOPH SCHREUER, PRINCIPLES OF INTERNATIONAL INVESTMENT LAW 61 (2d ed. 2012).

155 *Id.* at 63.

156 These limiting, "objective" requirements have also been applied by some tribunals to the more expansive definitions of investment in investment treaties as well. *See, e.g.*, Romak S.A. v Uzbekistan (Switz. v. Uzb.), PCA Case No AA280, Award, ¶ 207 (Nov. 26, 2009).

"Salini" criteria in the abstract;[157] whether they will be satisfied in the context of any particular data-related investor will depend heavily on the specific nature of that claimed investment. However, given the generally expansive statements by tribunals, the ICSID requirements for an investment might ultimately be readily fulfilled even by investors in businesses relying heavily on cross-border data transfer.

2 Investment "in the Territory of the Host State"

Apart from requiring an investment, treaties also frequently require that the investment be made "in the territory of" the host state.[158] In the context of businesses relying on data transfer, this requirement is likely to be difficult to separate from the fundamental requirement of an "investment." The territorial requirement is connected to the basic (though sometimes elusive) distinction between trade and investment. Broadly speaking, while cross-border traders operate from their home state even if selling goods or services into another state, cross-border investment by its nature involves more integration of business operations within the host state. For this reason, without an investment in the host state's territory, the would-be investor—such as a company simply offering products or services for sale over the Internet to consumers in another country—risks being viewed instead as a mere trader, and thus ineligible to access investment treaty protection.

> In the view of the *Bayview v Mexico* tribunal,
> it is quite plain that [the North American Free Trade Agreement] Chapter Eleven was not intended to provide substantive protections or rights of action to investors whose investments are wholly confined to their own national States, in circumstances where those investments may be affected by measures taken by another NAFTA State Party.[159]

Grand River Enterprises v USA also held that NAFTA did not protect investments located in the investor's home state even where those investments had been affected by measures taken

---

[157] Salini Costruttori S.P.A. v. Morocco (It. v. Morocco), ICSID Case No. ARB/00/4, Decision on Jurisdiction, ¶ 52 (July 23, 2001), 42 ILM 609 (2003).

[158] CAMPBELL MCLACHLAN, LAURENCE SHORE & MATTHEW WEINIGER, INTERNATIONAL INVESTMENT ARBITRATION: SUBSTANTIVE PRINCIPLES 180 (2007).

[159] Bayview Irrigation District v Mexico (U.S. v. Mex.), ICSID Case No. ARB(AF)/05/1, Award, ¶ 103 (June 19, 2007).

by authorities in another state.[160] Similarly, in another NAFTA case, *Apotex v USA*, the tribunal found that preparatory work completed in Canada by the Canadian claimant to meet U.S. pharmaceutical regulations (in order to sell the products within the US) did not count as an investment in the U.S. The tribunal characterized Apotex's operations as consisting of extensive investments in its home state of Canada, where its products were produced, but as merely cross-border trade when these products were exported to the U.S. Even the presence of a U.S.-registered subsidiary based in Delaware, which served as a U.S. distributor for the parent company's products, did not convince the tribunal that there was an investment in the U.S. Instead, the U.S. activity and the Canadian expenditures "simply supported and facilitated its Canadian-based manufacturing and export operations."[161]

The businesses that rely most heavily on cross-border data transfer in their operations are likely to be found in the technology sector. However, it is also this sector that is perhaps least likely to have a physical presence in the countries in which it is able to operate, precisely because many of its products and services can be delivered electronically via the Internet. A company such as Dropbox, for instance, providing "cloud" data storage facilities to individuals and businesses, can offer its services to any Internet user worldwide, relying on the possibility of transfer of the user's data out of its home state and to Dropbox's servers in the U.S. [162] Indeed, in February 2016, Dropbox reported that around 75% of its users were based outside the U.S.[163] Even if Dropbox's operations amount to an "investment" *per se*, it may be more difficult to conclude that they amount to an investment in the territory of any of the states of those non-U.S. users.

Such tech companies do, however, sometimes maintain offices outside their home state to engage in activities related to the core business, including marketing and business development. Dropbox itself has recently opened offices in Europe, Japan, and Australia for these purposes.[164] In many

---

160 Grand River Enterprises Six Nations Ltd v USA, UNCITRAL, Award, ¶ 87 (Jan. 12, 2011).

161 Apotex Inc v. USA, UNCITRAL, Award on Jurisdiction and Admissibility, ¶ 235 (June 14, 2013).

162 *Where Does Dropbox Store My Data?*, DROPBOX, www.dropbox.com/en/help/7.

163 Thomas Hansen, *Dropbox is Growing in Europe*, DROPBOX BUSINESS BLOG (Feb. 11, 2016), blogs.dropbox.com/business/2016/02/dropbox-is-growing-in-europe.

164 Stuart Dredge, *Dropbox Opens London Office and Buys Israeli Mobile Startup CloudOn*, *The Guardian*, (Jan. 22, 2015), www.theguardian.com/technology/2015/jan/22/dropbox-london-office-cloudon-windows-phone; Thomas Hansen, *Dropbox is Growing in Europe*, DROPBOX BUSINESS BLOG (Feb. 11, 2016), blogs.dropbox.com/business/2016/02/dropbox-is-growing-in-europe.

cases, tribunals have been content to rely on the fact that the claimant owned shares (even a minority share) in a company incorporated in the host state. Given that investment treaties commonly define investment to include shares in a company,[165] the equity interest in the local company—often a subsidiary investment vehicle specifically incorporated to conduct the particular investment in the host state—is frequently considered sufficient to meet the definition of investment under the relevant IIA.[166] Thus, marketing offices maintained by data companies might assist in finding not only an investment, but also an investment in the territory of the host state.

Moreover, other tribunals have favored a holistic analysis to determine whether there is an investment in the territory of the host state. For the *CSOB v Slovakia* tribunal, for instance, "it was irrelevant whether particular aspects of an investment were not performed within the territory of the host State."[167] Instead, what was important was that the claimant's activity as a whole constituted an investment, with sufficient connection to the host state to allow the territorial element to be fulfilled. [168] The exact degree of host state connection required was addressed in *SGS v Philippines*. In that case, despite the fact that the claimant's services were largely provided outside the Philippines, the tribunal emphasized (amongst other factors) the existence of a "liaison office" in Manila, employing a large number of people and substantially coordinating the claimant's operations. [169] The *SGS* tribunal concluded that, taken together, a "substantial and non-severable aspect of the overall service was provided in the Philippines."[170] Other cases, such as *Fedax v Venezuela*, have suggested the need for a benefit to the host state, even if the investment operations do not physically occur in the host state.

Meanwhile, the *LESI v Algeria* tribunal noted that "[n]othing prevents investments from being committed in part at least from the contractor's home country but in view of and

---

165 *See, e.g.*, Agreement Between The Government of the Republic of India and the Government of the United Kingdom of Great Britain and Northern Ireland for the Promotion and Protection of Investments art 1(b)(ii), Mar. 14, 1994, www.finmin.nic.in/bipa/United%20Kingdom.pdf..

166 For one recent example, see Kristian Almås and Geir Almås v. Poland, UNCITRAL, Award, ¶ 201 (June 27, 2016).

167 Christina Knahr, *Investments "In the Territory" of the Host State*, *in* INTERNATIONAL INVESTMENT LAW FOR THE 21ST CENTURY: ESSAYS IN HONOUR OF CHRISTOPH SCHREUER 49 (Christina Binder, Ursula Kriebaum, August Reinisch & Stephan Wittich eds., 2009).

168 Ceskoslovenksa Obchodni Banka, A.S. v. Slovakia, ICSID Case No. ARB/97/4, Decision of the Tribunal on Objections to Jurisdiction, ¶ 89, (May 24, 1999).

169 SGS Société Générale de Surveillance S.A. v. Philippines (Switz. v. Phil.), ICSID Case No. ARB/02/6, Decision on Jurisdiction, ¶ 101 (Jan. 29, 2004).

170 *Id.* at ¶ 102.

as part of the project to be carried out abroad."[171] The tribunal added that preparatory spending and other intangible contributions are often made in an investor's home state, but are "no less destined for the country concerned [*i.e.*, the host state]." Although the *LESI* case related to a construction contract, these comments are generalizable to other investments as well, and would support data-related investments with a less substantial connection to the host state than more traditional investments such as in manufacturing or agricultural industries. Furthermore, the *EMV v Czech Republic* tribunal confirmed that a foreign investor's contract with a local partner in the Czech Republic amounted to an investment in Czech territory. The contract related to the transfer of broadcasting rights, conferred by Czech authorities under statute, from a Czech individual to the claimant. For the tribunal, such a contract was "firmly anchored within the territory of the Czech State."[172] Such views could support data companies with similarly intangible rights by virtue of a contract with a partner in the designated host state.

B Core Obligations: No Obvious Breach But Case-Dependent

1 No Indirect Expropriation

For a claimant that manages to demonstrate the existence of an investment in the host state's territory, the next hurdle will be proving a violation of one of the guarantees of the relevant investment treaties. Amongst the guarantees typically found in IIAs, the protection against indirect expropriation is likely to be prominent in any claim. An investor affected by a state restriction on data transfer may seek to argue that the restriction amounts to an indirect (or regulatory) expropriation for which compensation is due. The definition of indirect expropriation has, of course, long remained controversial. Debates persist over whether a merely adverse effect on the investor is sufficient to constitute an expropriation, or whether an (possibly disguised) intention to expropriate on the part of the state is required. Where the effect on the investor is emphasized, it is not clear what degree of adverse effect is demanded to cross the threshold from routine, non-compensable regulation to impermissible regulatory expropriation. A common formulation used in the

---

171 LESI SpA v. Algeria (It. v. Alg.), ICSID Case No. ARB/05/3, Decision, ¶ 73 (July 12, 2006).

172 European Media Ventures SA v. Czech Republic, UNCITRAL, Partial Award on Liability, ¶ 38 (July 8, 2009).

case law, however, is that a "substantial deprivation" of the investment will amount to an expropriation.[173] The proportionality of the measure and the investor's "reasonable, investment-backed" expectations may also be relevant to the determination in some circumstances. These latter two factors may be particularly relevant where the case is heard under a more recent investment treaty that includes an interpretive Annex on indirect expropriation, such as treaties concluded by the U.S. since the 2003 U.S.-Singapore Free Trade Agreement[174] and U.S.-Chile Free Trade Agreement.[175]

Under a test of "substantial deprivation," at least some of the measures most likely to be taken by states in the area of data transfer may not cross the threshold to amount to expropriation. The most prominent recent development in the area, for instance, is the October 2015 decision of the European Court of Justice to strike down the "Safe Harbor" agreement, under which the personal data of EU citizens was permitted to be stored in the U.S., as discussed above. Depending on the implementation of the Privacy Shield (noted earlier), EU states may be forced to impose data localization requirements—*i.e.*, a requirement to store data on servers physically located within the EU—on companies dealing with the data of EU citizens. These requirements will undoubtedly interfere with the operations of businesses like Dropbox and its competitor Box, which rely heavily on cross-border data transfer. However, both Dropbox and Box have already taken steps towards reorienting their business operations to store data locally (*i.e.*, within the EU).[176] The industry generally appears to have treated new data localization requirements as merely a new headache to deal with, rather than a fundamental shift in their operations or a destruction of their ability to continue in business.[177] On this view, data localization requirements are not likely to constitute substantial deprivations. Similarly, a requirement to gain additional, stronger consent from users before transferring their data outside their home state is likely to be construed as relatively minimal, and not sufficiently onerous to amount to expropriation.

Restrictions or additional requirements placed on cross-border data transfer might alternatively fall within the so-

---

173 DOLZER & SCHREUER, *supra* note 154, at 104.

174 United States-Singapore Free Trade Agreement, May 6, 2003, ustr.gov/trade-agreements/free-trade-agreements/singapore-fta/final-text.

175 United States-Chile Free Trade Agreement, June 6, 2003, ustr.gov/trade-agreements/free-trade-agreements/chile-fta/final-text.

176 Hansen, *supra* note 165; Hayley Tsukayama, B*ox Teams Up with IBM and Amazon to Solve a Major Data Storage Problem*, WASH. POST (Apr. 12, 2016), www.washingtonpost.com/news/the-switch/wp/2016/04/12/box-teams-up-with-ibm-and-amazon-to-solve-a-major-data-storage-problem/.

177 The situation could, however, be different for smaller enterprises, less able to bear the costs of data localisation.

called "police powers" of the state. The doctrine of police powers, now well accepted in international law,[178] suggests that, as the *Methanex* tribunal put it "non-discriminatory regulation for a public purpose, which is enacted in accordance with due process . . . is not deemed expropriatory."[179] A tribunal might view such restrictions, particularly where aimed at maintaining privacy, national security, or public morals, merely as ordinary laws falling within the host state's power to regulate. Naturally, much will depend on the nature of the exact measure at issue in a case.

2 Fair and Equitable Treatment

The fair and equitable treatment (FET) obligation is also likely to be relevant to an investment treaty claim relating to data transfer, as it is in nearly every investment treaty claim. As with indirect expropriation, the precise meaning of the obligation is a matter for debate, with numerous entire monographs dedicated to the question in recent years.[180] Many tribunals and commentators agree, however, that the concept of legitimate expectations has "generally been considered central in the definition of the FET standard, whatever its scope."[181] On this view, states will breach FET if they resile from expectations created by specific representations made to an investor regarding a particular matter.[182] The FET standard is also often applied to matters of process, including the manner in which states pass new laws or take executive action. In this sense, FET is allied to concepts such as transparency, due process, good faith, non-discrimination, and non-

---

178 "[S]upport for the police powers doctrine appears to be overwhelming." UNCTAD, *Expropriation* 85 (UNCTAD/DIAE/IA/2011/7, July 2012).

179 Methanex Corporation v. USA, UNCITRAL, Final Award of the Tribunal on Jurisdiction and Merits, pt IV ch D ¶ 7 (Aug. 3, 2005),. For a recent application of the police powers doctrine, see Quiborax S.A. v Bolivia (Chile v. Bol.), ICSID Case No. ARB/06/2, Award, ¶¶ 201-27 (Sept. 16, 2015).

180 *See, e.g.*, I Tudor, *The* Fair and Equitable Treatment Standard *in the International Law of Foreign Investment* (OUP 2008); M Paparinskis, *The International Minimum Standard and Fair and Equitable Treatment* (OUP 2013); A Diehl, *The Core Standard of International Investment Protection: Fair and Equitable Treatment* (Kluwer 2012); R Kläger, *'Fair and Equitable Treatment' in International Investment Law* (CUP 2011).

181 Oxus Gold v. Uzbekistan, UNCITRAL, Award, ¶ 313 (Dec. 17, 2015). *See, e.g.*, Michele Potestà, *Legitimate Expectations in Investment Treaty Law: Understanding the Roots and the Limits of a Controversial Concept*, 28 ICSID REV. 88 (2013).

182 DOLZER & SCHREUER, *supra* note 154, at 145; CAMPBELL MCLACHLAN, LAURENCE SHORE & MATTHEW WEINIGER, INTERNATIONAL INVESTMENT ARBITRATION: SUBSTANTIVE PRINCIPLES 235 (2007).

arbitrariness.[183] FET is not completely inflexible; tribunals have acknowledged that "[n]o investor may reasonably expect that the circumstances prevailing at the time the investment is made remain totally unchanged."[184] The obligation may also depend on the particular situation of the host state in question, with less developed states potentially given some leeway in their adherence to ideal FET principles.[185]

Measures taken against particular Internet services, such as the ban imposed on Twitter by Turkey in 2014,[186] issued at short notice and with arguably political motives,[187] may fall foul of FET obligations. Wholesale, drastic changes in the applicable legal framework relating to data transfer or Internet use might also violate FET. Given the breadth of the FET standard, though, it is difficult to make general pronouncements about its application in the data transfer context.

3 Non-Discrimination

Investment treaties also provide guarantees of non-discrimination to foreign investors. These guarantees (in particular, the national treatment and most-favored-nation guarantees) protect investors against discrimination on grounds of nationality. Agreements between particular states or groupings to bypass privacy restrictions in place for other countries, such as the EU-U.S. Safe Harbor and Privacy Shield agreements, could potentially raise similar questions of discrimination under investment law as analyzed above under trade law. However, non-discrimination guarantees in investment treaties do not necessarily protect against

---

183 *See, e.g.*, Electrabel, S.A. v Hungary (), ICSID Case No. ARB/07/19, Decision on Jurisdiction, Applicable Law and Liability, ¶ 7.74 (Nov. 30, 2012); McLachlan et al., *supra* note 183, at ch. 7, §2(A).

184 Saluka Investments BV v. Czech Republic (Neth. v. Hung.), UNCITRAL, Partial Award, ¶ 305 (Mar. 17, 2006). More recently, the *Philip Morris v Uruguay* tribunal observed that, "generally, there must be a reasonable expectation of regulation": Philip Morris Brands Sàrl v. Uruguay (Switz. v. Uru.), ICSID Case No. ARB/10/7, Award, ¶ 269 (July 8, 2016); *see also id.* at ¶¶ 422-25.

185 Houben v. Burundi (Belg. v. Burundi), ICSID Case No. ARB/13/7, Award, ¶¶ 185-88 (Jan. 12 2016); Nick Gallus, *The Influence of the Host State's Level of Development on International Investment Treaty Standards of Protection*, 6 J. OF WORLD INV. & TRADE 711 (2005).

186 *Twitter website 'blocked' in Turkey*, BBC NEWS (Mar. 21, 2014), www.bbc.com/news/world-europe-26677134; *Turkey Twitter ban: Constitutional court rules illegal*, BBC NEWS (Apr. 2, 2014), www.bbc.com/news/world-europe-26849941.

187 According to the BBC, the ban was imposed following allegations of corruption made on Twitter against the Turkish Prime Minister and his inner circle. *Twitter website 'blocked' in Turkey*, *supra* note 188.

differential treatment based on other grounds apart from nationality. In certain markets relevant to cross-border data transfer, such as the market for Internet search or social media websites, there may effectively be only one participant. Any state measure aimed at the Internet search market, for instance, might appear to be a measure targeted at the single participant in that market; if that participant is foreign-owned, the measure may appear to be discriminatory. A tribunal may nevertheless find that the measure is designed to meet a justifiable regulatory need in the Internet search market, and that the fact that its adverse effects are borne largely (or entirely) by a foreigner does not suffice to make the measure discriminatory. The *Clayton/Bilcon v Canada* NAFTA tribunal, for instance, recently held that states can "pursue reasonable and [facially] non-discriminatory domestic policy objectives through appropriate measures even when there is an incidental and reasonably unavoidable burden on foreign enterprises."[188] The existence of any local comparators in "like circumstances," as the requirement is often phrased in investment treaties, and the tribunal's position on whether a discriminatory intent against the foreigner is needed,[189] will likely play a large role in any claim of discrimination in relation to data transfer policies.

C Key Exceptions

Even if a tribunal finds a breach of an investment treaty protection, the state may nevertheless escape responsibility by means of an exceptions clause in the relevant treaty, or (perhaps) by means of the customary international law defense of necessity.

1 General Exceptions: More Restricted Than in the Trade Context

Very few bilateral investment treaties contain general exceptions clauses that cover all (or most) obligations in the treaty, similar to GATT art XX or GATS art XIV, as discussed above. However, such clauses are appearing more frequently in recent treaties. A review by UNCTAD of investment agreements signed during 2014, for instance, noted that a general exceptions clause was found in fourteen of the eighteen treaties in the sample, while the equivalent survey of treaties

---

188 Clayton v. Canada (U.S. v. Can.), PCA Case No. 2009-04, Award on Jurisdiction and Liability, ¶ 723 (Mar. 17, 2015).

189 DOLZER & SCHREUER, *supra* note 154, at 203.

signed during 2013 similarly located the clause in fifteen out of eighteen agreements.[190]

Where a general exceptions clause does exist, it typically clarifies that host states' obligations to protect investors do not prevent the states from taking measures necessary to achieve certain specified objectives. The relevance of a general exceptions clause to an investment claim relating to data transfer therefore depends on whether states are likely to justify interferences with cross-border flows of data by reference to any of those specified objectives. As mentioned earlier, the objectives most likely to be supported by such interferences are national security, public morals or public order, and privacy. However, general exceptions clauses in investment treaties usually list health and environmental objectives, sometimes including protection of artistic treasures and public morals or public order as well. Depending on the content of the data being transferred, the public morals objective could justify interferences, for instance with Internet-based businesses relating to gambling or pornography. [191] Privacy, on the other hand, does not feature in the list; the specific exception related to privacy in GATS art XIV(c)(ii) is replicated only in a few IIAs that incorporate that provision by reference.[192] National security also does not feature amongst the enumerated objectives (although—as discussed below—it appears relatively often in a separate, specific exception clause). Because of this, general exceptions clauses as currently drafted may not play a significant role in data-related investment claims.

2 Exceptions for National Security: Rare and Uncertain Application to Data Transfer

Investment treaties do, however, occasionally contain specific exceptions for national security. Certain prominent multilateral treaties, including NAFTA and the *Energy Charter Treaty*,[193] include a provision permitting a state party to take any action "that it considers necessary for the protection of its

---

190 UNCTAD, WORLD INVESTMENT REPORT 2015: REFORMING INTERNATIONAL INVESTMENT GOVERNANCE 112 (2015) 112; UNCTAD, WORLD INVESTMENT REPORT 2014: INVESTING IN THE SDGS – AN ACTION PLAN 116 (2014).

191 See the discussion of "public morals" above in section IIIA5.

192 Panama-Taiwan Free Trade Agreement, Aug. 21, 2003, www.sice.oas.org/trade/panrc/panrc_e.asp; China-New Zealand Free Trade Agreement, Apr. 7, 2008, www.mfat.govt.nz/en/trade/free-trade-agreements/free-trade-agreements-in-force/china-fta/text-of-the-new-zealand-china-fta-agreement/.

193 Energy Charter Treaty,,34 ILM 360, opened for signature Dec. 17, 1994, entered into force Apr. 16, 1998, www.energycharter.org/process/energy-charter-treaty-1994/energy-charter-treaty/ [hereinafter ECT].

essential security interests."[194] In one well-known example from a bilateral treaty, art XI of the bilateral investment treaty (BIT) between the U.S. and Argentina reads: "This Treaty shall not preclude the application by either Party of measures necessary for the maintenance of public order, the fulfillment of its obligations with respect to the maintenance or restoration of international peace or security, or the protection of its own essential security interests."[195]

As noted earlier, states may seek to justify restrictions on cross-border data transfer on the grounds that national security would be imperiled if foreigners gained access to certain crucial data. A foreign-owned software company operating in a host state might develop new encryption techniques, for example, that it wishes to export to third states. The host state might, however, object to the transfer of any code containing the new encryption techniques to certain "hostile" states, since this might interfere with the effectiveness of the host state's espionage activities against the hostile states. The host state's concern in this scenario would lie not with any imminent or actual military invasion or violent attack, but with a longer-term, more diffuse risk that its security could be undermined.

A question arises as to whether a national/essential security clause in an investment treaty would capture this kind of security threat. Indeed, it has been argued that the essential security clause covers only situations of "significant militaristic threat,"[196] thus being unlikely to justify preventive restrictions on data transfer. In the *Oil Platforms* case, the International Court of Justice (ICJ) placed an essential security clause in the context of the use of force and self-defense,[197] suggesting that long-term or non-specific risks to security may not be covered by the exception. In the version of the clause found in NAFTA, application is expressly limited to situations of arms traffic, a "time of war or other emergency in international relations," or non-proliferation of nuclear weapons, none of which would appear to relate to the restrictions on data transfer envisaged here.[198]

Other versions of the security exception, such as art XI of the USA-Argentina BIT, are not so expressly limited, and have been applied in situations beyond military invasion and

---

194 NAFTA art. 2102; ECT art. 24.

195 United States-Argentina Bilateral Investment Treaty, Nov. 14, 1991, 2001-2009.state.gov/documents/organization/43475.pdf.

196 William J. Moon, *Essential Security Interests in International Investment Agreements,* 15 J. OF INT'L ECON. L. 481, 499 (2012).

197 Oil Platforms *(*Iran v. U.S.*)*, Judgment, 2003 I.C.J. Rep. 161, ¶ 78 (Nov. 6)..

198 ECT art. 24 contains a similar list of categories of essential security interests; although, it is only illustrative (rather than exclusive, like NAFTA), since it is introduced with the word "including."

violence. Many of the well-known Argentina cases, for instance, applied the clause to an economic crisis, with one tribunal commenting:

> If the concept of essential security interests were to be limited to immediate political and national security concerns, particularly of an international character, and were to exclude other interests, for example major economic emergencies, it could well result in an unbalanced understanding of Article XI. Such an approach would not be entirely consistent with the rules governing the interpretation of treaties.[199]

Indeed, restrictions on data transfer in the interests of national security would arguably be closer to the intent of the essential security clause than the restrictions on currency convertibility adopted by Argentina and sought to be justified under the same clause. Even if the clause is not taken to be "self-judging," it is by no means inconceivable that a tribunal might interpret the clause to cover restrictions on data transfer.

Nevertheless, while the security exception might be more common than a general exception, it is still far from ubiquitous. A 2007 OECD study of 43 countries' BIT programs found that 39 countries included no security exception at all. Where the exception did exist, it was sometimes limited to particular obligations such as expropriation.[200] The more usual situation for states, then, is that no exceptions clause will be available to justify restrictions on data transfer on grounds of either privacy or national security. States' defenses will therefore be likely to focus on arguments that their measures did not constitute violations of investment treaty obligations in the first place.

3 The Customary Defense of Necessity: A High Threshold

The potential relevance of the customary international law defense of necessity must also be considered in this context. This defense sits alongside any treaty-based defenses such as the exceptions clauses just considered, and may provide an additional avenue by which states can escape responsibility for an interference with a data investor's rights. However, it is often recognized that the customary defense is difficult to satisfy, intended only for extreme cases.

---

199 CMS Gas Transmission Company v. Argentina (U.S. v. Arg.), ICSID Case No. ARB/01/8, Award, ¶ 360, May 12, 2005.

200 Katia Yannaca-Small, *Essential Security Interests under International Investment Law* , *in* International Investment Perpsectives: Freedom of Investment in a Changing World 98 (2007) www.oecd.org/investment/internationalinvestmentagreements/40243411.pdf.

In particular, as codified in the International Law Commission's Articles on State Responsibility, the defense contains two requirements that may prove to be sticking points for states seeking to rely on it in this context. Firstly, the state must be facing a "grave and imminent peril."[201] As noted above, the kinds of risks to national security that would justify limitations on cross-border data transfer are not likely to amount to grave and imminent perils, instead being more diffuse, longer-term risks. It is true that the ICJ recognized, in the *Gabcikovo-Nagymaros* case, that "a 'peril' appearing in the long term might be held to be 'imminent' as soon as it is established, at the relevant point in time, that the realization of the peril, however far off it might be, is not thereby any less certain and inevitable."[202] However, the indication that the peril must still be "certain and inevitable" might limit the usefulness for states of this view, since threats to national security are most likely described in terms of risks rather than certainties. Secondly, the state's response to the peril must be "the only way" for the state to protect itself.[203] Again, this is difficult to prove, since states usually have a wide range of possible actions at their disposal to respond to any given situation.[204] The success of the claim is likely to depend on the particular reasons for which the state is seeking to limit data transfers in the case at hand.

D Specific Rules on Data Transfer in the TPP: Inapplicable

As discussed above, the TPP and some other recent preferential trade agreements (PTAs), including investment chapters contain particular language relevant to data transfer. Under TPP art 14.13.2, for example, states parties must not impose requirements on investors to use or locate computing facilities within a host state as a condition for conducting business in the state. TPP art 14.11.2 imposes a more general obligation for states parties to "allow the cross-border transfer of information by electronic means, including personal information," for the business purposes of a foreign investor. However, these obligations are unlikely to be directly relevant

---

201 *Articles on Responsibility of States for Internationally Wrongful Acts* art 25(1)(a). [2001] 2 Y.B. Int'l L. Comm'n, U.N. Doc. A/56/49(Vol. I)Corr.4, legal.un.org/ilc/texts/instruments/english/draft_articles/9_6_2001.pdf,

202 Gabcikovo-Nagymaros Project (Hung. V. Slovk.), Judgment, 1997 I.C.J. Rep. 7, ¶ 54 (Sept. 25).

203 *Articles on Responsibility of States for Internationally Wrongful Acts*, *supra* note 202, at art. 25(1)(a).

204 The *Continental Casualty* tribunal acknowledged this, effectively finding that the "only way" requirement could be read as the "only *reasonable* way" for a state to achieve its objective: Continental Casualty Company v. Argentina (U.S. v. Arg.), ICSID Case No. ARB/03/9, Award, ¶¶ 192-98 (Sept. 5, 2008).

to a claim by an investor under the investment protection provisions in TPP ch 9. Those provisions only allow TPP investment tribunals to rule on claimed breaches of the substantive investment obligations in ch 9 itself.[205] An investor could not therefore claim that a state had breached the obligation to allow cross-border data transfer in art 14.11.2. Instead, the investor would be confined to claiming that a restriction on cross-border data transfer constituted, for instance, an expropriation or a breach of FET in violation of TPP arts 9.6 or 9.7.

Nevertheless, TPP ch 14 does provide some comfort to investors in its treatment of the interaction between Chapters 9 and 14. While arts 14.11.3 and 14.13.3 contain exceptions to states' obligations on data transfer and data localization, an "exception" to the exceptions is effectively contained in TPP art 14.2, which provides that states' obligations on data transfer and data localization are subject to the investment obligations in Chapter 9. This means that, even when a state invokes the exceptions in Chapter 14 (perhaps citing concerns of privacy or national security), it may not have breached Chapter 14, but its conduct can still be tested against the strictures of Chapter 9 in a claim by an investor. The state would then need to demonstrate that its conduct did not breach an investment protection obligation, or to rely on an alternative exceptions clause, such as the security exception in TPP art 29.2. As a result, though, the TPP's innovative provisions on data transfer are not likely to feature in investment claims.

V REFORMING TRADE AND INVESTMENT LAW TO FACILITATE DATA TRANSFERS: NORMATIVE ISSUES AND POLICY OPTIONS

The previous sections of our paper highlight various legal uncertainties and complications in relation to the application of international trade and investment law to data transfer. In this section, we turn our attention to normative and policy reforms within these regimes that may help facilitate data transfer. In order to maintain integrity and trust in the global Internet, data transfers must be not only free and open, but also secure and efficient. In practice, however, achieving openness, efficiency and security simultaneously can be challenging. As discussed in part II, this challenge is already evident in the tussle between countries regarding the extent to which governments should control cross-border data

[205] TPP art. 9.18. This provision also permits tribunals to hear claims for breaches of investment authorisations or investment agreements, but such claims are not relevant for present purposes.

flows to implement policy goals such as privacy, cybersecurity or public order. Several questions remain unanswered, including the appropriate standards and benchmarks applicable to issues of consumer trust such as privacy and cybersecurity, the extent to which governments should censor online content to preserve public morality or order, and when such policy measures simply constitute disguised protectionism.

To achieve the goal of open, free and efficient data flows, reformulation or creative interpretation of existing trade and investment disciplines is necessary, in light of the realities of the information economy. In order to synergize trade and investment disciplines on data transfer with each other, and with other facets of the information economy, policy-makers will need to engage at two levels, to: (a) bring about necessary legal and policy reforms within the individual areas of international trade and investment law (what we term *internal engagement*); and (b) coordinate and engage with disciplines and institutions outside trade and investment law that impact data flows (what we term *external engagement*). While the political and cultural divide between countries on issues such as privacy, censorship and surveillance will continue to pose obstacles to a unified approach, this dual-pronged engagement is likely to result in greater coherence in trade and investment disciplines on data transfer.

A Internal Engagement: Creating Synergies in Trade and Investment Disciplines

In the existing structure of trade and investment agreements, the legitimacy of policy measures restricting data transfer may fall to be determined under exceptions clauses (such as GATS art XIV or art XIV *bis*, or a general exception or security exception clause in a BIT).[206] Particularly in applying GATS art XIV and similarly worded general exceptions, tribunals have considerable discretion in assessing the legality of a data transfer-restrictive measure. As discussed earlier in part IIIA5, these exceptions entail stringent standards, and several kinds of measures restricting data transfer, including privacy and consumer protection measures, may fall afoul of the GATS. For example, tribunals may find that: certain administrative requirements are applied in a discriminatory

[206] *See generally* Shin-yi Peng, *Cybersecurity Threats and the WTO National Security Exceptions*, 18 J. OF INT'L ECON. L. 449 (2015). Note, however, that general exceptions clauses are not as common in IIAs.

manner;[207] the restriction fails to contribute to the policy goal, such as preventing the public circulation of certain prohibited material or protecting security of data; [208] or alternative measures are available that are more effective in achieving data security and privacy, such as implementing stronger encryption standards.[209]

However, tribunals may lack the requisite knowledge of foundational issues such as the efficacy of technical standards on security and privacy, the economic impact of data transfer restrictions, and the technical feasibility and reliability of proposed alternative measures. Further, no international consensus currently exists on cybersecurity standards and privacy principles. Tribunals will therefore need to rely on economic and technical evidence for the development of future jurisprudence on exceptions clauses and their applicability to data transfer issues. For example, a tribunal could consider economic and technical evidence, where available, on whether domestic servers are more secure or provide better economies of scale, or whether a government can regulate online content in accordance with its public morality without the need for large-scale website blocking. Since the wording of exceptions clauses typically predates the digital age, the existing jurisprudence may become less relevant.

Even with the assistance of evidence from experts, the complex technical nature of data flows and the dearth of economic evidence on data transfer mean that tribunals are likely to falter while balancing liberalization of data flows with security and privacy. This deficiency indicates the need for policy-makers to consider alternative tools to achieve the desired balance between openness in data flows and maintaining security and consumer trust. We have already discussed in part IIIB how the TPP prohibits data localization (TPP art 14.11) and mandates the free flow of information (TPP art 14.13), as well as requiring TPP parties to adopt a legal framework for protection of personal information (TPP art 14.8). The TPP's future may be uncertain, but some of these rules are likely to spill over to other ongoing negotiations such as TTIP and TiSA. These new-generation agreements, therefore, may offer more specific provisions to deal with some of the uncertainty in applying international trade and investment law to data transfer measures. These specific provisions allow countries to agree in advance on which restrictions are acceptable and which are not, instead of

---

207 For instance, a requirement to register websites with a local authority, or to obtain a domestic license to host content, may be comparatively more burdensome for foreign service providers.

208 See text accompanying n. 38.

209 Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 INT'L J. OF COMM. 2221, 2230 (2016).

leaving the difficult balancing to be conducted by WTO panels or investment tribunals on a case-by-case basis.

Given the centrality of issues of privacy, cybersecurity and consumer protection in digital data flows and in digital trade more broadly, these legal initiatives in the Electronic Commerce Chapter of the TPP are welcome. Other trade and investment agreements should aim to provide more legal avenues to recognize the importance of these policy measures at multilateral, regional, and bilateral levels. At the multilateral level, a separate annex on electronic commerce might be developed under the GATS, incorporating principles to facilitate free, efficient, and secure data flows. Alternatively, new provisions on domestic regulation in the electronic commerce sector might be developed under GATS art VI, setting out how fundamental principles on data transfer could be implemented. Finally, provisions on secure and free data transfers might also be directly incorporated in trade and investment agreements through explicit provisions, as in the case of recent mega-regional FTAs.

Another important legal reform is to build synergies in the interpretation of international trade law and international investment law, such that the legal outcomes under these two disciplines are better aligned. As it stands, international trade and investment law disciplines may apply differently to identical measures restricting cross-border data transfer, for example when comparing an investor-state claim under an IIA with a state-state claim under the WTO or, perhaps, the TPP. First, as discussed in part IVA, putative investments engaging in cross-border data transfer will not necessarily have a sufficient connection with their host state to qualify as protected investments. Meanwhile, this threshold requirement does not pose a problem for a claim by a WTO Member under general GATS provisions (which could arise under modes other than mode 3) or a claim by a TPP party under specific e-commerce provisions. Second, international trade law and international investment law do not typically contain the same exceptions or deal in the same way with policy objectives typically underlying data transfer restrictions, such as national security, public morals, public order, and privacy. Aside from explicit exceptions, which may be differently worded in the contexts of trade and investment or play different roles in these two contexts, implicit flexibilities may also differ. For example, unlike WTO panels, investment treaty tribunals may potentially draw on the doctrine of police powers to grant flexibility in connection with substantive investment obligations, given that these obligations have developed largely in the absence of explicit exceptions.

Although the treaty language in trade and investment agreements is not necessarily identical, lessons may still be

drawn from jurisprudence in the investment context for the trade context, and vice versa. The significance of and need for such references between the fields is likely to increase as treaty practices develop. For example, as general exceptions based on GATT art XX and GATS art XIV become more common in IIAs, the WTO jurisprudence on these exceptions—including concepts of public morals and public order—may become more relevant to certain claims and defenses in investment treaty arbitration. Conversely, a future dispute involving GATS art XIV *bis* could lead a panelist, arbitrator, or Appellate Body Member in a trade dispute to have reference to discussions of "essential security interests" in investment treaty arbitration. Further, trade and investment obligations are being increasingly integrated in new-generation agreements such as the TPP and TTIP. These obligations will need to apply in a coherent fashion to measures restricting data transfer, precluding divergent legal outcomes in relation to data transfer measures within the two fields.

B External Engagement: Achieving Coherence with Other Disciplines

Although international trade and investment law are becoming increasingly important in regulating data transfers, these regimes themselves do not provide sufficient normative principles and policy solutions to deal with all legal issues related to data transfer. In order to resolve legal inconsistencies or ambiguities within trade and investment disciplines on data transfer (such as the interpretation and application of exceptions clauses), external engagement with institutions, and rules from outside trade and investment law may be necessary. In particular, normative principles in Internet policy-making provide an important tool for making new rules and interpreting existing rules in trade and investment agreements. For example, the principle of net neutrality (allowing non-discriminatory access to all content on the Internet, irrespective of who provides the content) is important in enabling innovation and providing opportunities to all service providers regardless of their country of origin or economic size. Similarly, the OECD Principles for Internet Policy Making seek to reconcile the free global flow of information with privacy protection and Internet security.[210]

In seeking greater clarity in trade and investment rules on data transfer, policy-makers can engage with external

---

[210] OECD, OECD PRINCIPLES FOR INTERNET POLICY MAKING 5-6, 11-12, 14-15 (2014) https://www.oecd.org/sti/ieconomy/oecd-principles-for-internet-policy-making.pdf,.

bodies through various mechanisms. At the stage of drafting of new rules on data transfer within trade and investment agreements, participating governments can invite comments from the Internet community after publicly releasing position papers or early drafts. The ongoing work on data protection, privacy, and cybersecurity at institutions such as the OECD, APEC, UNCTAD, the International Conference of Data Protection and Privacy Commissioners, and the Internet Governance Forum would also be useful guidance in the formulation of new disciplines in trade and investment agreements. Other policy initiatives from industry and civil society may assist in resolving issues with respect to data transfer. For example, a process of data classification based on the security and sensitivity levels of personal information, advocated by Microsoft, may be more workable than a blanket ban on data transfer.[211] Similarly, voluntary commitments from companies, through programs such as the Global Network Initiative, will be instrumental in maintaining the integrity and efficiency of data transfers, while respecting local norms and basic human rights.[212] Another positive industry mechanism is the publication of Internet transparency reports by Facebook, Google, Apple, Microsoft, and others, which outline government requests for user data, thus creating greater awareness of government surveillance activities.

Trade and investment agreements are not the appropriate platform to set overly specific standards on technical issues, such as cybersecurity, or to govern domestic policy issues, such as privacy or consumer protection. Yet, given the importance of the Internet in the global trade regime, trade and investment agreements must provide adequate "regulatory preconditions" to enable secure and open digital data flows. Rules requiring the free flow of information and the adoption of privacy laws, and the prohibition of data localization as in the TPP, are an example of this. Moving forward, trade and investment agreements can provide greater clarity to data transfer rules by including references to high-level principles without setting any specific standards. A comparable example is the presence of high-level principles on prudential regulation found in the recent FTA between Canada and the EU.[213] Clarity on such principles can facilitate mutual

---

211 *See, e.g.*, MICROSOFT INC,, A CLOUD FOR GLOBAL GOOD: A POLICY ROADMAP FOR A TRUSTED, RESPONSIBLE, AND INCLUSIVE CLOUD 49 (2016), https://news.microsoft.com/cloudforgood/_media/downloads/a-cloud-for-global-good-english.pdf.

212 *See, e.g.*, GLOBAL NETWORK INITIATIVE, PRINCIPLES ON FREEDOM OF EXPRESSION AND PRIVACY https://globalnetworkinitiative.org/principles/index.php.

213 Comprehensive Economic and Trade Agreement between Canada and the European Union, revised text released by the European Commission, Feb. 29,

recognition agreements between countries on privacy or cybersecurity, some of the main barriers to free data flows.

These developments, inspired by work done outside the typical trade and investment fora, can feed into the content of future such agreements, and also into tribunals' deliberations on the application of exceptions clauses or on doctrinal flexibilities in connection with substantive obligations.

VI CONCLUSION

Trade and investment disciplines can support data transfer by interpreting existing rules in the context of a broader policy goal of open, secure, and efficient data flows. A similar approach is warranted in the formulation of new disciplines on data transfer in the new-generation FTAs. By including more specific provisions to assist in liberalizing data flows, agreements such as the TPP, if implemented, will provide an important platform for building policy coordination and consensus within and between governments on some of these issues with respect to trade and investment. However, on their own, and with the existing exceptions for particular countries and references to international standards that have not yet been fully developed, they are not enough.

A major challenge facing governments today is to balance the liberalization goals of trade and investment agreements with the much broader goals of digital data management, including promoting domestic policy goals unrelated to trade and investment. The changing nature of investments and trading patterns in the modern-day information economy needs to be better understood and incorporated within both international trade law and international investment law, in order to support liberalization and growth of the digital sector. Quantitative and qualitative evidence on the link between data flows, productivity, innovation, and digital trade will help build a better framework for policies on data transfer. [214] Further, greater policy coherence is needed on a broad range of issues, including cybersecurity and data protection.

The legal outcomes arising from the application of international trade and investment law to issues of data transfer do not necessarily align with each other. Despite the different wording of trade agreements and investment agreements, though, the jurisprudence developed in each discipline may begin to influence the other, particularly in the

---

2016 (signed Oct. 30, 2016, not yet in force) , Annex XX of the Financial Services Chapter, High Level Principles.

[214] OECD, *Economic and Social Benefits of Internet Openness* 14 (Background Paper for Ministerial Panel 1.1, DSTI/ICCP(2015)17/FINAL, June 2, 2016).

interpretation of exceptions. For new-generation agreements, where trade and investment disciplines appear to be converging, the need to achieve harmony on data transfer is growing. Coordination between trade and investment law will help facilitate other developments such as e-commerce, cloud computing, and 3D printing.

Although trade and investment law have a significant role to play in facilitating the free flow of data, they cannot address all of the complex issues arising from cross-border data transfer. The development of further legal principles and policies in respect of cross-border data transfer will need support not only from governments and trade and investment regimes, such as the WTO and TPP, but also from other international bodies dealing with broader internet governance issues, as well as industry and consumers. Trade and investment agreements have the potential to encourage the adoption of more transparent and predictable practices on data transfer, as well as enhanced cooperation in developing appropriate legal frameworks. At the same time, stakeholders in the private sector and civil society will be critical in establishing appropriate technical standards and related rules and principles, policy, and practice.