1-2017

The legality of data residency requirements: How can the trans-pacific partnership help?

Shin-yi PENG

Han-wei LIU
Singapore Management University, hanweiliu@smu.edu.sg

The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?

Article *in* Journal of World Trade · April 2017

DOI: 10.54648/TRAD2017008

2 authors, including:

Han-Wei Liu
Monash University (Australia)
32 PUBLICATIONS **269** CITATIONS

SEE PROFILE

The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?

Shin-yi PENG* & Han-wei LIU**

Article 14.13 of the Trans-Pacific Partnership (TPP) Agreement – the data localization (DL) clause – represents the first time that a far-reaching preferential trade agreement (PTA) seeks to reduce protectionism arising from data residency (DR) requirements. The DL clause, however, is linked to a loose GATT Article XX-like exception: Article 14.13(3)(b), which allows the parties to maintain DR measures to achieve a legitimate public policy objective as long as the measure in question can satisfy the 'necessity test'. The ambiguity of the DL exception will be clarified by TPP tribunals when a real dispute occurs. After examining the rationales of the DR measures in the context of the necessity test, we find that the responding party invoking a DL exception will have strong arguments, especially when defending Types II and III of the DR measures. Arguments could be made that there is a genuine relationship between the ends, i.e. privacy protection, and the means, i.e. the DR measures. In addition, the responding party invoking a DL exception in a potential dispute would undoubtedly argue that the Mutual Legal Assistance Treaty (MLAT) cannot qualify as a 'genuine alternative', because the proposed measure must not only be 'less trade restrictive' than the DR measures, but should also 'preserve for (the responding party's) right to achieve its desired level of protection' with respect to law enforcement or a criminal investigation. Based upon our findings, we argue that with regard to Trade in Services Agreement (TiSA) and Transatlantic Trade and Investment Partnership (TTIP) negotiations on e-commerce, the major challenge of trade negotiators is the disciplinary fragmentation of global economic regulation. The DR issues in question confirm that international economic law (IEL) correlates to other areas of law. Future negotiations require more collaborative and interdisciplinary solutions through productive dialogue with experts in private international law and criminal procedure law. True and substantial changes in the theories and practices of Internet jurisdiction would allow us to argue for a more narrow interpretation of the DL exception – rendering it more difficult to satisfy the necessity test.

* Professor of Law, National Tsing Hua University, Taiwan. sypeng@mx.nthu.edu.tw

** Assistant Professor of Law, National Tsing Hua University, Taiwan. han-wei.liu@graduateinstitute.ch

An earlier version of this article was presented at *the Society of International Economic Law (SIEL) 5th Biennial Global Conference: International Economic Law in a Diverse World*, Johannesburg, South Africa, on 7–9 July 2016. We thank Amy Porges, Tania Voon, Bryan Mercurio, Heng Wang, Krista Schefer, and other conference participants for their comments. This article was accepted on 26 September 2016. Although the Trump Administration's withdrawal from the TPP in January 2017 essentially collapsed this mega-FTA, the manner in which it manages cross-border data flow, in our view, may still shed light on future negotiations.

Peng, Shin-yi & Liu, Han-wei. 'The Legality of Data Residency Requirements: How Can the Trans-Pacific Partnership Help?'. *Journal of World Trade* 51, no. 2 (2017): 183–204.

1 INTRODUCTION: A NEW BATTLEGROUND FOR INTERNATIONAL ECONOMIC LAW

The much-awaited text of the Trans-Pacific Partnership (TPP) Agreement was released in late 2015.[1] The TPP, often dubbed a 'high quality, twenty-first century' trade deal, casts a wide net by encompassing most of the critical issues that have emerged in the context of both the World Trade Organization (WTO) and preferential trade agreements (PTAs).[2] Robust online business transactions led TPP parties to reach beyond traditional market access in goods and services by establishing ground rules on electronic commerce in Chapter 14. As part of its core functions, this chapter seeks to prevent the open Internet from disintegrating into 'multiple, balkanized networks in which data flows are more expensive and more frequently blocked'.[3] Toward this end, and more specifically, the chapter contains three disciplines addressing the linkage between digital trade and information flow. Article 14.8 underscores the role of personal data protection by encouraging TPP parties to adopt measures in a manner that is in harmony with one another and consistent with the principle of non-discrimination. Article 14.11 requires TPP parties to ensure free information flow, 'when the activity is for the conduct of the business of a covered person'.[4] Finally, and perhaps the most innovative discipline, is Article 14.13, which we refer to as the data localization (DL) clause. This clause generally prohibits parties from mandating firms to 'use or locate computing facilitates' in their territory 'as a condition to conduct business'.[5] These three provisions, in conjunction with other rules in the same chapter, set forth a framework to ensure the cross-border transfer of data to facilitate e-commerce.[6] The DL provision – the focal point of this article – represents the first time that a mega PTA has explicitly touched upon DL or data residency (DR) issues.[7]

For years, regulatory intervention in the transnational information flow has been a source of controversy among the international economic law (IEL)

---

1 *See generally* the Text of the Trans-Pacific Partnership, The Office of the United States Trade Representative, https://ustr.gov/tpp/#text (accessed 30 Apr. 2016) [hereinafter the TPP Agreement].

2 *See* e.g. C. L. Lim, Deborah K. Elms & Patrick Low, *What Is 'High-Quality, Twenty First Century' Anyway?,* in *The Trans-Pacific Partnership: A Quest for a Twenty-First-Century Trade Agreement* (C. L. Lim, Deborah K. Elms & Patrick Low eds, Cambridge: Cambridge University Press 2012).

3 Chapter Summary: Ch. 14- Electronic Commerce, the Officer of the United States Trade Representative, https://medium.com/the-trans-pacific-partnership/electronic-commerce-87766c98a068#.m7mlqn618 (accessed 30 Apr. 2016).

4 TPP Agreement, *supra* n. 1, Art. 14.11.

5 *Id.*, Art. 14.13, paras 2–3.

6 *See* e.g. *Id.,* Art. 14.8.

7 Japan-Mongolia Economic Partnership Agreement, signed in 2015, also contains similar provisions. *See* Agreement Between Japan and Mongolia for an Economic Partnership, 10 Feb. 2015, Art. 9. 12.

community and information technology (IT) sectors.[8] This has been particularly true in recent years. DR requirements – measures that restrict the ability of companies to transfer data or more narrowly, as elaborated below, require local storage within a particular national border – are on the rise, both within and without the TPP.[9] TPP parties such as Australia, Brunei, Canada, Peru, New Zealand, Malaysia and Vietnam have in one way or another imposed limitations on data leaving their territories, which have in turn affected data processing and global trade.[10] Beyond the TPP, similar regulatory initiatives can be found in various developed and developing countries, including Brazil, China, the European Union (EU), India, Russia, South Korea and Taiwan, to name just a few.[11] Whatever the differences between these DR measures, their economic impacts clearly extend far beyond the IT industry itself, implicating global welfare.[12] While the goal of the TPP drafters is to address the potential ramifications of DR requirements through the above new disciplines, their effectiveness as a legal tool in resolving digital trade concerns remains unsettled.

For instance, the DL provision does not foreclosure DR altogether. Rather, it follows the path laid out under Articles 14.8 and 14.11 by allowing intervention as long as relevant measures 'do not constitute arbitrary or unjustifiable discrimination and are not more restrictive than necessary to achieve legitimate policy objective'.[13] Thus, while the TPP seeks to balance trade and non-trade concerns in a digital setting, questions remain: Why do states regulate cross-border information flow, or even mandate the location in which data can be stored and processed? What are the underlying rationales of these DR measures: public interest, protectionism, or both? Can DR be justified from a trade law perspective, and if so, to what extent? What represents the possible yardstick against which one may detect protectionism under the guise of legitimate public

---

8 *See* Rolf Weber, *Legal Safeguards in Cloud Computing*, in *Privacy and Legal Issues in Cloud Computing*, 25–30 (Weber et al. eds, Cheltenham/Northampton 2015).

9 For the purpose of this article, data residency or data localization is loosely defined as measures controlling over the location where regulated data physically reside. Conceptually, DR requirements can be seen as a sub-set of the so-called forced localization measures (FLMs). For the present purpose, we focus on DR, while acknowledging the growing concerns about other FLMs. For discussions of other FLMs in the TPP, *see* e.g. Han-Wei Liu, *The Political Economy Behind the Encryption Clauses in the TPP Agreement*, 51(2) J. World Trade (2017).

10 Albright Stonebridge Group, *Data Localization: A Challenge to Global Commerce and the Free Flow of Information*, www.albrightstonebridge.com (accessed 5 May 2016).

11 *Id.*, at 5.

12 It is reported that GDP of Brazil, China, and EU, for instance, would suffer losses by -0.2%, -1.1%, and -0.4%, respectively, as a result of recently introduced or proposed DR legislations. *See generally* Matthias Bauer et al., *The Costs of Data Localisation: Friendly Fire on Economy Recovery* (ECIPE Occasional Paper No. 3/2014), www.ecipe.org/app/uploads/2014/12/OCC32014__1.pdf (accessed 5 May 2016).

13 TPP Agreement, *supra* n. 1, Art. 14.13.

policies? Finally, how, in the end, can the TPP resolve growing concerns regarding digital protectionism?

This article seeks to address these questions using a threefold approach, which is structured as follows. First, we contextualize emerging concerns by documenting and categorizing various legal approaches to DR adopted by both TPP and non-TPP parties (section 2). Second, we explore an area that remains largely unaddressed among cyberlaw scholars,[14] economists,[15] and trade lawyers[16] by critically reviewing DR-related provisions found in the TPP. Specifically, we discuss the DL clause and its 'public policy objectives' exception by examining these issues in the context of the necessity test (section 3). Third, we conclude by generalizing our findings to inform trade negotiations in, among other agreements, the Trade in Services Agreement (TiSA) and the Transatlantic Trade and Investment Partnership (TTIP) (section 4).

Before we begin our inquiry, some caveats are in order. First, while our main focus is on Chapter 14, other TPP chapters are also relevant here, including Chapter 10, among others.[17] Second, despite the new rules found in Chapter 14, the TPP adopts a more relaxed approach in Chapter 11 (Financial Services). Although this approach has frustrated industry stakeholders – notably the US, who called upon trade negotiators to fix the loophole[18] – it is a matter of policy debate in the financial sector that extends beyond the scope of this article. With all of this in mind, we now embark on our inquiries.

2 RECENT LEGAL DEVELOPMENTS OF DATA RESIDENCY: THE TPP AND BEYOND

Countries adopt various legal approaches to control trans-border information flow, depending upon their unique economic, social and political structure. While some

---

14 Iva Mihaylova, *Could the Recently Enacted Data Localization Requirements in Russia Backfire?*, 50 J. World Trade 313 (2016); Anupam Chander & Uyên P. Lê, *Data Nationalism*, 64 Emory L.J. 677 (2015).

15 Bauer et al., *supra* n. 12.

16 Daniel Crosby, *Analysis of Data Localization Measures Under WTO Services Trade Rules and Commitments*, E15 Initiative, International Center for Trade and Sustainable Development (ICTSD) and World Economic Forum (2016).

17 The DR requirements affecting services delivered electronically could come under the ambit of Ch. 10. Thus, while this limited space bars us from undertaking a detailed examination of all possible provisions applicable to DR, it would be remiss not to consider certain disciplines in Ch. 10 to the extent that they are relevant to the above-mentioned anti-protectionism instruments.

18 Concerns over this carve-out has led to some proposals from the US to add new clauses in the TPP to prohibit regulators from imposing DR requirements on financial service companies. However, as Deputy U.S Trade Representative Robert Holleyman suggests, it is problematic to 'take bits and pieces of TPP and reopen it for negotiation', these concerns are most likely to be addressed in future trade negotiations. *See Holleyman: TPP Financial Services Fix Balances Interests of Congress, Regulators*, World Trade Online (10 June 2016).

of these measures generally follow the traditional model of privacy protection, others are more intrusive, requiring the (re)location of computing facilities. Whatever the approach used, many of these measures appear to run counter to the underlying logic of the Internet by transforming a borderless cyberspace into 'balkanized' units, which in turn affect the digital economy. To appreciate the implications of such measures on global trade, we illustrate the overall trend in cross-border data flow by assessing the situation and, more crucially for analytical purposes, by classifying the various regulatory approaches of select TPP and non-TPP parties.

2.1 Regulatory approaches to cross-border data flow

2.1[a] *TPP Members*

Both developed and developing countries within the TPP have introduced DR in some form. In one area of the developed world, Australia has proven pioneering among its counterparts. Data privacy in Australia is generally subject to the Privacy Act 1988,[19] as amended by the Privacy Amendment (Enhancing Privacy Protection) Act 2012.[20] Australian Privacy Principles (APPs) are created as part of these amendments, and these principles set forth how public and private sectors manage personal data.[21] Under APP 8.1, no entity is allowed to disclose personal information to an overseas recipient unless reasonable steps – such as enforceable contracts – are taken to ensure that an overseas recipient does not breach the APPs.[22] However, this restriction does not apply to cases in which an overseas recipient is governed by a law 'substantially similar' to the APPs; informed consent is obtained from the data subjects; or the disclosure of data is otherwise permitted by Australian law or a court order.[23] To further complicate the matter, in addition to data privacy rules of general application, Australia has adopted the Personally Controlled Electronic Health Records Act 2012 (PCEHR).[24] Section 77 of the PCEHR lays down a requirement 'not to hold or take records outside Australia'. In effect, the PCEHR prohibits any Australian electronic health records from

---

19 Privacy Act 1988 (Australia). In Australia, data protection is governed by federal, state, and territory legislations. For a background, *see* e.g. Greg Tucker, *Frontiers of Information Privacy in Australia*, 63 J. L. & Info. Sci. 70–80 (1992).

20 Privacy Amendment (Enhancing Privacy Protection) Act 2012 (Australia).

21 The APPs replace both the Information Privacy Principles and the National Privacy Principles. *See* Privacy Fact Sheet 17, Office of the Australian Information Commissioner, https://www.oaic.gov.au/individuals/privacy-fact-sheets/general/privacy-fact-sheet-17-australian-privacy-principles (accessed 18 May 2016).

22 Privacy Act 1988 (Australia), Schedule 1– Australian Privacy Principles 8.1 [hereinafter APP].

23 *Id.*, APP 8.2.

24 Personally Controlled Electronic Health Records Act 2012 (Australia) [hereinafter PCEHR].

being stored outside Australia. Such requirements essentially force multinational enterprises that manage health-related data to either maintain local data centres or outsource to firms that reside in Australia.[25]

Comparable measures can be found throughout the developed world. In Canada, for instance, cross-border data flow is subject to the Personal Information Protection and Electronic Documents Act (PIPEDA), which contains requirements similar to APP 8.1.[26] While this federal law does not require the maintenance of computing facilities in Canada, certain provinces have adopted localization mandates: British Columbia[27] and Nova Scotia,[28] for instance, require personal data held by public institutions or a third party on their behalf to be stored and accessed in Canada, with a select few exceptions. Despite their potential implications for digital trade, such measures have been fashioned from the DL clause contained in the TPP, a phenomenon that will be addressed later in this work.

DR requirements are also pervasive in certain areas of the developing world. In this regard, Malaysia appears to have taken the lead by enacting the 'Personal Data Protection Act' (PDPA) in 2010.[29] With a few exceptions, Article 129 of the PDPA prohibits transfer of 'any personal data of a data subject to a place outside Malaysia'.[30] Vietnam followed suit in 2013 by issuing the 'Decree on Management, Provision, and Use of Internet Services and Information Content Online', known as 'Decree 72'.[31] This controversial order bans the online sharing of materials that harm 'national security, social order, and safety' and also requires Internet service providers to have at least one local server to facilitate the 'inspection, storage, and provision of information' upon the request of competent authorities.[32]

---

25 M. James Daley et al., *The Impact of Emerging Asia-Pacific Data Protection and Data Residency Requirements on Transnational Information Governance and Cross-Border Discovery*, 16 Sedona Conf. J. 201, 216 (2015). *See also* Chander & Lê, *supra* n. 14, at 683.

26 Personal Information Protection and Electronic Documents Act (2000), as amended on 23 June 2015 (Canada).

27 Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165 (Canada) [hereinafter FIPPA]. S. 30.1 of the FIPPA reads: 'A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada' unless the informed consent is obtained from the data subject or the relevant jurisdiction where the information is stored is permitted for the purpose of the FIPPA, or other conditions set out under s. 33.1 of the FIPPA.

28 Personal Information International Disclosure Protection Act, S.N.S. 2006 (Canada).

29 Personal Data Protection Act 2010 (Malaysia) [hereinafter PDPA]

30 *Id*., s. 129.

31 Decree on Management, Provisions and Use of Internet Services and Online Information (Decree 72/2013/ND-CP) (Vietnam), http://www.moit.gov.vn/Images/FileVanBan/_ND72-2013-CPEng.pdf (accessed 22 May 2016) [hereinafter Decree 72]. Decree 72 has received harsh criticisms from the human rights groups for limiting freedom of the social media users and the press. *See* e.g. Peter Shadbolt, *Rights Groups Take Aim at Vietnam's New Internet Laws*, *CNN* (2 Sept. 2013), http://edition.cnn.com/2013/09/02/world/asia/vietnam-internet (accessed 22 May 2016).

32 *Id*., at Art. 24.

2.1[b] *Non-TPP Members*

Beyond the TPP, legal developments in the BRIC countries (Brazil, Russia, India and China) and Europe are noteworthy in our discussions on the existing DL provision, as well as future trade negotiations, in light of their sheer market power.

In Brazil, the Marco Civil da Internet (Marco Civil) has been under consideration by Congress since 2009. The legislation is designed to protect the fundamental rights of Internet users and to ensure, among other considerations, net neutrality, freedom of access and speech, and data privacy.[33] On data protection, more specifically, Article 11 of the draft bill required that the process of collection, storage, custody, and treatment of personal data shall follow Brazilian laws, while Article 12 contained a DL requirement.[34] Industry pressure stripped Article 12 from the final law, which was passed on 23 April 2014.[35] It has been reported, however, that the Brazilian government is considering the reinstatement of local server requirements by introducing the 'Data Protection Law'.[36] Moreover, while Article 12 was removed, Article 11 remained in placed in the final legislation. Therefore, firms that deal with Brazilian user information bear legal risks for noncompliance with Brazilian data protection laws.[37]

Additionally, in 2011 the Indian Ministry of Communication and Information Technology promulgated the IT Rules. Transnational data transfer is prohibited unless the data recipient is subject to the same level of protection as required under the Rules, and unless such transfer is necessary in the performance of the lawful contract or the consent of the data subject is obtained.[38] While India's IT Rules do not contain a DL mandate, India's National Security Council (NSC) has begun the process of proposing a new policy that would require Indian data to be stored locally.[39]

---

[33] For a background, *see* e.g. Jonah Force Hill, *The Growth of Data Localization Post-Snowden: Analysis and Recommendations for US Policymakers and Industry Leaders*, 2 Lawfare Research Paper Series 1, 16–19 (2014).

[34] Art. 12: 'The Executive Branch, through Decree, may force connection providers and Internet applications providers (… omitted) to install or use structures for storage, management and dissemination of data in the country (omitted)'. Substitutivo ao Project de Lei n. 2126 de 2011, English translation by Carolina Rossini, http://www.ip-watch.org/2013/11/14/desperate-final-stretch-for-the-marco-civil-do-brasil/ (accessed 23 May 2016).

[35] Allison Grande, *Brazil Nixes Data Localization Mandate from Internet Bill*, Law360, http://www.law360.com/articles/520198/brazil-nixes-data-localization-mandate-from-internet-bill (accessed 24 May 2016).

[36] Hill, *supra* n. 33, at 18.

[37] Lei No. 12.965, de 23 Abril de 2014, Diário Oficial da União [D.O.U.] de 24 Apr. 2014 (Brazil).

[38] The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules (India) [hereinafter India IT Rules].

[39] Thomas K. Thomas, *National Security Council Proposes 3-Prolonged Plan to Protect Internet Users*, Hindu BusinessLine (13 Feb. 2014), http://www.thehindubusinessline.com/info-tech/national-security-council-proposes-3pronged-plan-to-protect-internet-users/article5685794.ece (accessed 24 May 2016).

The desire for DR is alive in two additional BRIC countries as well. In China, cross-border data flow is subject to several overarching instruments and various sector-specific rules. The Law on Guarding State Secrets, as amended in 2010, prohibits data from being removed from China if it is deemed a 'state secret', including 'matters that have a vital bearing on state security and national interests'.[40] In 2011 and 2014, China adopted the Information Security Technology Guidelines for Personal Information Protection within Public and Commercial Services Information Systems and the Counter-terrorism Law, respectively: the former serves as a voluntary standard, discouraging transnational data flow without a data subject's consent or regulatory approval,[41] while the latter requires telecommunications companies and Internet service providers to preserve relevant records.[42] Regarding sector-specific rules, DL restrictions apply to, for instance, the health[43] and banking industries.[44]

Russia is perhaps the most aggressive among the BRIC countries in the development of a comprehensive framework on DL. The Russian legislature passed Federal Law No. 242-FZ (a DL law) by requiring a data operator to ensure that the collection, recording, systematization, accumulation, storage, updating, amending, and retrieval of any information about Russian citizens must be done via servers located in its territory and that competent authorities must be notified regarding the location of storage facilities where such data is stored.[45] While the

---

40 Zhong hua ren min gong he guo bao shou guo jia bi mi fa [The Law of the People's Republic of China on Guarding State Secrets] (promulgated by the Standing Committee of the National People's Congress, 5 Sept. 1988, as amended on 29 Apr. 2010).

41 Xin xi an quan ji shu – gong gong ji shang yong fu wu xin xi xi tong ge ren xin xi bao hu zhi nan [Information Security Technology – Guidelines for Personal Information Protection within Public and Commercial Services Information Systems] (promulgated by the Standardization Administration and General Administration of Quality Supervision, Inspection and Quarantine of the Republic of China, 5 Nov. 2012).

42 Zhong hua ren min gong he guo fang kong bu zhu yi fa [Counter-territorial Law of the People's Republic of China] (promulgated by the Standing Committee of the National People's Congress, 27 Dec. 2015).

43 Zhong hua ren min gong he guo ren kou jian kang xin xi guan li ban fa (shi xing) [Population Health Information Management (Pilot)] (promulgated by the National Health and Family Planning Commission, 5 May 2014) (which prohibits the storage of personal health information in overseas data centres).

44 *See* e.g. Guan yu ying hang ye jin rong ji gou zuo hao ge ren jing rong xí bǎo hù gōng zuò de tōng zhī [Notice to Urge Banking Financial Institutions to Protect Personal Information] (promulgated by the People's Bank of China, 20 Jan. 2011) (requiring that personal financial information should be stored and processed in China, unless applicable laws provide otherwise).

45 Federal Statute of 5 May 2014 No.97-FZ 'On Amendments to the Federal Statute 'On Information, Information Technologies and on the Protection of Information' and Specific Legal Acts of the Russian Federation on the Issues of Regulation of Information Exchange with the Use of Telecommunication Networks' Ros. Gaz., No.101, (7 May 2014), www.rg.ru/2014/05/07/inform tech-dok.html (accessed 25 May 2015). For a detailed account of Russia's Blogger's Law and other major amendments to information law, *see generally* Andrei Richter &Anya Richter, *Regulation of Online Content in the Russian Federation: Legislation and Case Law* (Strasbourg: European Audiovisual Observatory 2015). For an overview of the Data Localization Law, *see* e.g. Mihaylova, *supra* n. 14,

Russian regulator sought to downplay the implications of the law by clarifying that major targets would most likely be 'organizations with a physical presence in Russia (which can be subject to on-premise audits)' and 'organizations that direct Internet activity to Russian users (whose websites can be blocked by the regulator', the scope of application is far from settled given the nature of the Internet.[46] Together, these DR requirements may significantly undermine online activities and e-commerce and have been subject to criticism both at home and abroad.

In the EU, DL requirements have been at the forefront of the debates. For decades, cross-border data transfer has been subject to the 1995 Data Protection Directive, which prohibits information from moving out of the region unless the destination country maintains adequate protection as provided in the EU.[47] However, the revelations of the U.S. National Security Agency (NSA) have in some ways overhauled the EU's data protection regime. First, the EU-U.S. Safe Harbour – a scheme that enabled American firms to transfer data from the EU to the US – was invalidated by the European Court of Justice in 2015[48] and was subsequently replaced by the EU-U.S. Privacy Shield.[49] The Privacy Shield, though not yet in effect, imposes new safeguards to ensure European citizens the same data protection when data is processed in the US Second, and more profoundly, the 1995 Data Protection Directive is being repealed by the General Data Protection Regulation (GDPR).[50] The GDPR, like its predecessor, restricts the ability of firms to move personal data to a non-EU country unless such a transfer is made to an adequate jurisdiction or a derogation applies.[51] While the application of

---

at 315–317; Dmitry Kurochkin et al., *Russia's New Server Localization Law: Implications for Foreign Companies*, 15(2) Bloomberg BNA: World Data Protection Report (2015).

46 Natalia Gulyaeva et al., *Russia Update: Regulator Publishes Data Localization Classifications*, Hogan Lovells (11 Aug. 2015), http://www.hldataprotection.com/2015/08/articles/international-eu-privacy/russia-update-regulator-publishes-data-localization-clarifications/ (accessed 25 May 2016).

47 Directive 95/46/EC of the European Parliament and the Council of 24 Oct. 1995 on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data, Art. 25 [hereinafter 1995 Data Protection Directive]. *See* Commission Decision on the Adequacy of the Protection of Personal Data in Third Countries, http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm (accessed 25 May 2016).

48 Case C-362/14, *Maximillian Schrems v. Data Protection Commissioner*, 6 Oct. 2015 (the Court declared the Safe Harbour agreement invalid by pointing out the US failed to offer adequate protection given the surveillance by the US intelligence agencies).

49 Fact Sheet, *EU-U.S. Privacy Shield* (Feb. 2016), http://ec.europa.eu/justice/data-protection/files/factsheets/factsheet_eu-us_privacy_shield_en.pdf (accessed 25 May 2016).

50 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 Apr. 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General Data Protection Regulation). For an overview of the reform, *see* Reform of EU Data Protection Rules, European Commission, http://ec.europa.eu/justice/data-protection/reform/index_en.htm (accessed 25 May 2016).

51 Binding corporate rules and model contract, for instance, are alternative mechanisms for cross-border transfer. *Id.*, Art. 44–49.

the GDPR is pending until 25 May 2018, certain Member States, both collectively and separately, are already dedicated to the new DR requirements.

Led by France and Germany, several European countries have been considering the so-called 'Schengen Routing' system to restrict Internet traffic within the boundaries of the Schengen area.[52] Respectively, France and Germany have also considered new rules which would mandate that data be stored in the nation. The French government, for instance, has expressed its preference for local storage.[53] Most recently, on 3 May 2016, France's lawmakers proposed a draft bill requiring the storage of personal data in data centres located in the EU and prohibiting information from leaving this region.[54] Likewise, Germany has since late 2011 begun to consider 'Bundescloud' (federal cloud) on the premise that such a facility would be safer than one exclusively controlled by a private entity.[55] In sum, while it remains to be seen whether the EU and its Member States would end up with naked DR that mirrors Russia's DL Law, it suffices to say that a rigorous scheme on international data flow is imminent.

2.2 Types of data residency requirements

We have so far outlined the widespread proliferation of regulatory restrictions on trans-border information flow. While these measures vary in both their scope and intensity, DR generally moves along the spectrum. For the convenience of

---

[52] *See* Daniel Dönni et al., *Schengen Routing: A Comparative Analysis*, in *Intelligent Mechanisms for Network Configuration and Security*, 100–101 (Steven Latré et al. eds, Cham, Switzerland: Springer International Publishing AG 2015). *See also* Laura K. Donohue, *High Technology, Consumer Privacy, and U.S. National Security,* 4 Am. U. Bus. L. Rev. 11, 21 (2015); *Schengen for Data: What is Necessary, What is Feasible*, United Clouds of Europe (29 Aug. 2014), https://www.fabasoft.com/en/group/newsroom/united-clouds-of-europe/archive/schengen-for-data-what-is-necessary-what-is-feasible (accessed 29 May 2016).

[53] Cloudwatt, a cloud-computing firm, with around 30% of shares being held by the French government, for instance, has been promoting local data storage. *See* e.g. Tatevik Sargsyan, *Data Localization and the Role of Infrastructure for Surveillance, Privacy, and Security*, 10 Int'l J. Comm. 2221, 2227 (2016).

[54] However, this proposed clause has raised questions about its compatibility with the GDPR. Myriam Gufflet, *French Senate Proposed Data Localization*, Privacy Tracker (12 May 2016), https://iapp.org/news/a/french-senate-proposes-data-localization/ (accessed 26 May 2016).

[55] Patrick S. Ryan et al., *When the Cloud Goes Global: The Global Problem with Data Localization*, 46(12) Computer 54, 57 (2013). It is reported that this initiative has been concretized as part of the consolidated plan to build up Germany's new IT infrastructure by 2022; this plan has raised concerns about the possible introduction of DR requirements that would undermine e-commerce. Monika Kuschewsky, *Data Localization Requirements Through the Backdoor? Germany's 'Federal Cloud', and New Criteria for the Use for Cloud Services by the German Federal Administration*, Inside Privacy (15 Sept. 2015), https://www.insideprivacy.com/cloud-computing/germanys-criteria-for-federal-use-of-cloud-services/ (accessed 27 May 2016); Chander & Lê, *supra* n. 14, at 692–693; Natalia Drozdiak, *Germany's Tough Line on Data Transfer to U.S. is Criticized*, Wall St. J. (29 Oct. 2015), http://blogs.wsj.com/brussels/2015/10/29/germanys-tough-line-on-data-transfers-to-u-s-is-criticized/ (accessed 26 May 2016).

discussion, we have divided these DR requirements into three types, as depicted in Figure 1 below.

At one extreme lies Type I, which takes the form of naked restraints by requiring personal data to be stored in facilities located within a specific jurisdiction. Type I is exemplified by measures adopted in China, Russia and Vietnam. At the other end of the spectrum is Type III, as currently adopted by the EU,[56] which limits the ability of companies to transfer data to a third country without requiring data to be kept for a certain period of time or in a particular place.[57] Somewhere in the middle are those measures introduced by Canada and Australia, referred to as Type II. While cross-border information flow under Type II is also subject to certain conditions (e.g. equivalent protection, consent of the data subject, etc.), hard-line local storage mandates apply only to specific types of data. An example of this can be found in regulations passed by British Columbia and Nova Scotia that require data held by the public sector to be stored and accessed in Canada, as well as Australia's PCEHR, which applies to electronic health records.

To be clear, however, while all of these measures could result in impacts on trade that vary in degree, certain Type I and Type II DR requirements are carved out from the TPP. First, Article 14.2(3) explicitly excludes 'government procurement' or 'information held or processed by or on behalf of a Party, or measures related to such information, including measures related to its collection' from the application of Chapter 14.[58] Thus, Canada's provincial laws will most likely be exempted from the DL clause.[59] Second, pursuant to TPP Articles 14.2(4) and 14.2(5),[60] DR requirements concerning the financial sector fall outside the DL clause.[61] Conceivably, TPP parties would be able to adopt what has been done in

---

[56] It should be noted that however the Schengen routing regime or Germany's Bundesloud, if effective, may arguably move the EU towards the Type I or Type II DR.

[57] Some refer to measures that require firms to keep data for a particular minimum period of time as 'data retention' requirements and those with local storage mandates as 'data residency'. *See* e.g. Lothar Determann et al., *Residency Requirements for Data in Clouds – What Now?*, Privacy and Security Law Report, http://www.globalequityequation.com (accessed 10 Sept. 2016).

[58] TPP Agreement, *supra* n. 1, Art. 14.3.

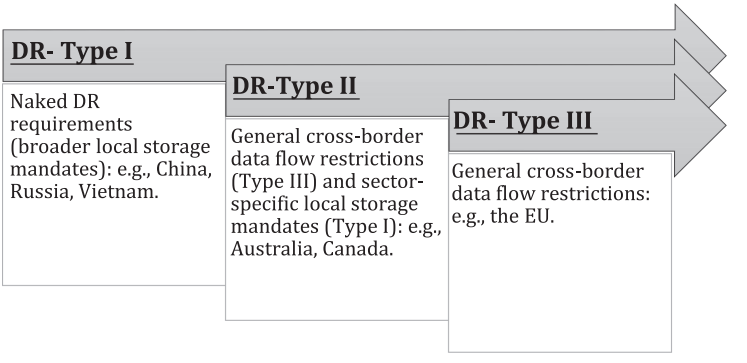
[59] In the same vein, measures that introduce the public cloud (e.g. Germany's proposed Bundescloud) would not be caught by the TPP's DL clause so long as they satisfy Art. 14.2.

[60] Cross-border financial data transfer is subject to, among other provision, Art. 11.6 and terms and conditions as laid down in each TPP member's commitment. Certain TPP members, including Canada, Chile, Peru, Singapore, Mexico, Malaysia, and Vietnam, has imposed additional restrictions on transfer and processing of financial data. Canada, for instance, adopts a sort of Type I DR by requiring that '*cross-border financial services supplier maintain a local agent and records in Canada*' (emphasis added). *See* TPP Agreement, Annex 11-A: Canada.

[61] Unlike Ch. 14, Ch. 11 does not have the DL clause. This carve-out has raised concerns about potential trade barriers. In Jan. 2016, a group of Congressmen from the US thus urged the Obama Administration to remove the exemption. *See* Mike Kelly et al., *Data Localization Letter to the Department of Treasury, the United States Trade Representative, and National Economic Council* (11 Jan. 2016), http://kelly.house.gov/(accessed 28 May 2016).

the banking industry in China. Whether or not these exceptions may provide a loophole for the purposes of protectionism is debatable and is also beyond the scope of this article. For this reason, discussions in section 3 will focus on the DR measures that arguably come under the aegis of the TPP. The questions facing us, then, are as follows: Can the TPP Agreement help to reverse the trend of DR, and if so, how?

Figure 1 Types of DR Requirements



3 THE LEGALITY OF DATA RESIDENCY MEASURES UNDER THE TPP

3.1 The data localization clause and its 'public policy' exception

Chapter 14 has three key clauses that address DR-related concerns: Article 14.13 is the core provision that specifically confronts naked DR measures (Type I),[62] while

[62] TPP Agreement, *supra* n. 1, Art. 14.13: Location of Computing Facilities:

(1) The Parties recognize that each Party may have its own regulatory requirements regarding the use of computing facilities, including requirements that seek to ensure the security and confidentiality of communications.

(2) 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.

(3) Nothing in this Article shall prevent a Party from adopting or maintaining measures inconsistent with para. 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 the use or location of computing facilities greater than are required to achieve the objective.

Articles 14.8 and 14.11 lay down general disciplines on personal data protection and cross-border information flow, which may apply to all three types of DR measures illustrated above. According to the United States Trade Representative (USTR), the DL clause in Chapter 14 of the TPP is structured to guarantee that 'companies will not have to build expensive and unnecessarily redundant data centres in every market they seek to serve'.[63] In economic terms,[64] free trans-border data flow would enable IT giants such as Google, Facebook and Amazon to build up their global network and data centres based on their business models, thereby increasing economic efficiency.[65] Yet data centres are capital-intensive. A leading firm's investment can yield direct benefits for the host state, including knowledge, skilled and relatively high-paying job opportunities, and taxes.[66] Indirectly, the localization of data indicates that the host state has a stable business and political environment, which would in turn attract more technology and skilled professionals.[67] Together, this may create the cluster effect, which supports the growth of the IT industry and, more broadly, data-related economic sectors of a nation.[68]

The TPP also seeks to reduce protectionism arising from various DR requirements. However, Articles 14.11 and 14.13 follow a similar vein by recognizing that the parties may have their own regulatory requirements concerning 'the transfer of information by electronic means',[69] as well as those governing 'the use of computing facilities'.[70] More specifically, the TPP Agreement allows parties to maintain a DR measure to achieve a legitimate public policy objective as long as the measure '*does not impose restrictions on the use or location of computing facilities greater than are required to achieve the objective*' (emphasis added).[71] In other words, while the mandate of each clause varies, what they have in common is that they all draw upon – among other anti-protectionism proxies – the necessity test.

To illustrate, the DL clause is linked to a loose GATT Article XX-like exception clause: Article 14.13(3)(b) (hereinafter the 'DL exception'). However,

---

63 USTR, *Chapter Summary of Electronic Commerce*, https://ustr.gov/sites/default/files/TPP-Chapter-Summary-Electronic-Commerce.pdf (accessed 10 Sept. 2016).

64 *See generally* Bauer et al., *supra* n. 12.

65 *See* e.g. Joshua Paul Meltzer, *The Internet, Cross-Border Data Flows and International Trade*, 2(1) Asia & Pac. Pol'y Stud. 90, 91–92 (2015).

66 Shamel Azmeh & Christopher Foster, *The TPP and the Digital Trade Agenda Digital Industrial Policy and Silicon Valley's Influence on New Trade Agreements* (LSE International Development Working Paper No.16-175), at 25, http://www.lse.ac.uk/internationalDevelopment/publications/Working-Papers/WP175-ShamelAzmeh.aspx (accessed 29 May 2016).

67 *Id*., at 27–28.

68 *Id*.

69 TPP Agreement, *supra* n. 1, Art. 14.11.

70 TPP Agreement, *supra* n. 1, Art. 14.13.

71 *Id*.

the DL exception differs from GATT/GATS general exceptions. In the latter, policy objectives are exhaustively listed, and the legitimacy of a measure is assessed in the light of these objectives. The TPP's DL exception contains an open-ended list of legitimate objectives and requires an initial determination regarding whether an objective is legitimate.[72] In fact, the drafting of the DL exception was intentionally loose in its approach. In the absence of such a vague exception, most TPP parties would not have made the positive commitments on data transfer and computing facilities.[73] TPP negotiators intentionally created this 'constructive ambiguity' and wrote ambiguously worded provisions in these politically sensitive areas.[74] Considering the high level of controversy surrounding the DR issues, leaving a DL clause vague may make sense, as it is practically necessary for parties to reserve the space to argue for various positions of law.[75] The 'ambiguity' of the DL exception, therefore, will be clarified by TPP tribunals when a real dispute occurs.

3.2 How can the TPP help? the necessity test

'Necessity tests', which are found in various treaties or in different provisions, must be read in context, and also in light of the object and purpose of the agreement concerned.[76] Nevertheless, we argue that a TPP tribunal may borrow the WTO's jurisprudence on the 'necessity test', simply because most legal authorities use the principle of proportionality when they must choose between competing values and interests.[77] In addition, Article 28.12 of the TPP also requires TPP panels to consider relevant interpretations in reports of the WTO panels and the Appellate Body with respect to any provision of the WTO Agreement that has been incorporated into the TPP.[78]

In this context, the Appellate Body in recent cases has identified certain principles in evaluating the contribution of a measure in the context of a necessity analysis under Article XX. The Appellate Body stressed that the selection of a methodology to assess a measure's contribution is a function of the nature of the

---

72 *See* Gilles Muller, *The Necessity Test and Trade in Services: Unfinished Business?* 49(6) J. W. T. 951, 959 (2015).

73 The Authors appreciate Amy Porges for sharing her insights and providing this viewpoints.

74 *See* Shin-yi Peng, *Regulating New Services Through Litigation?–Electronic Commerce as a Case Study on the Evaluation of 'Judicial Activism' in the WTO*, 48(6) J. World Trade 1189–1222 (2014).

75 *See* John H. Jackson, *Restructuring the GATT System* 51 (1990). Claus-Dieter Ehlermann, *Six Years of Bench of the World Trade Court*, 36(4) J. World Trade 635 (2002).

76 Panel Report, *Colombia – Measures Relating to the Importation of Textiles, Apparel and Footwear* (hereinafter *Colombia – Textiles*), WT/DS461/AB/R, 27 Nov. 2015, para. 7.304.

77 Muller, *supra* n. 72, at 958.

78 TPP Agreement, *supra* n. 1, Art. 28.12.

risk, the objective pursued, and the level of protection sought.[79] In this regard, the Appellate Body has consistently held that a contribution exists when there is a genuine relationship of ends and means between the objective pursued and the measure at issue.[80] The Appellate Body has further explained that in most cases, a comparison between the challenged measure and possible alternatives should be undertaken.[81]

The crux of the matter is the connection between the DR measures and the public policy objectives upon which the DR measures are based. What are the underlying rationales of the DR measures? What are the non-trade concerns at issue? Additionally, can such policy objectives be achieved through a less intrusive but equally effective measure?

3.2[a]. *Privacy and Security – Conflict of Laws*

The explosion in the volume of data collected and processed today is unprecedented.[82] The technological ability to collect, aggregate and process an ever-greater volume and variety of data continues to grow, which in fact means that we are now living in a world of ubiquitous data collection.[83] In the age of 'Big Data', wearable technologies with voice and video interfaces, combined with networked devices, are further expanding our capacity to collect information.[84] The wide variety of potential uses for big data analytics raises crucial questions primarily surrounding the question of how to protect privacy in this big data world.[85] The advancement of technology, and especially the development of cloud computing services, has changed the way data is stored by breaking down borders and expanding jurisdictional reach.[86] Under

---

79 Appellate Body Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products* (hereinafter *EC – Seal Products),* WT/DS400/AB/R, WT/DS401/AB/R, 18 June 2014, para. 5.210.

80 *See* e.g. *Colombia – Textiles, supra* n. 76, para. 7.310. *See also* Panel Report, *Argentina – Measures Relating to Trade in Goods and Services* (hereinafter *Argentina – Financial Services),* WT/DS453/AB/R9, May 2016, para. 7.684.

81 *EC – Seal Products*, para. 5.214.

82 Executive Office of the President, United States, *Big Data: Seizing Opportunities, Preserving Values* (2014), http://WhiteHouse.gov/BigData (accessed 17 June 2015).

83 Ann Cavoukian et al., *Privacy by Design in the Age of Big Data* (8 June 2012), https://privacybydesign.ca/content/uploads/2012/06/pbd-big_data.pdf (accessed 18 June 2015).

84 *Id*.

85 ITU, *2013 Big Data ITU-T Watch Report*, http://www.itu.int/ITU-T/techwatch (accessed 17 Sept. 2016). Executive Office of the President, United States, *Big Data: Seizing Opportunities, Preserving Values* (2014), http://WhiteHouse.gov/BigData (accessed 17 Sept. 2016). ICO (Information Commissioner's Office), UK, *Big Data and Data Protection* (28 July 2014), https://ico.org.uk/media/for-organisations/documents/1541/big-data-and-data-protection.pdf (accessed 17 Sept. 2016).

86 *See* Kate Westmoreland et al., *International Law Enforcement Access to User Data: A Survival Guide and Call for Action*, 13 Can. J. L. & Tech. 225, 230–245 (2015); Jennifer Daskal, *The UN-Territoriality of*

this trend,[87] users' privacy and information security are the most oft-cited rationale. Countries that justify themselves under such a policy framework include, Australia, China, the EU, Malaysia, Russia, and Vietnam.[88] For these countries, DR appears to offer an effective way to resolve privacy concerns.

At the core of the issue is the reality that Internet jurisdiction is an unsettled area of the law.[89] The Internet is global, while regulation thereof is local.[90] The fact that data is moving from one place to another renders such data subject to another jurisdiction's privacy laws.[91] In many cases, the dynamics of global data flows render it almost impossible to identify the location of personal data at any given moment, as well as which jurisdiction's laws should be applied.[92] Privacy regimes, however, vary considerably. Privacy laws that emerge from divergent cultures differ dramatically from country to country – spanning from the comprehensive to the nonexistent.[93] The lack of consistency among various national privacy statutes has created conflict of laws problems, especially when such data is transferred from a country with stronger data protection regulation to one with weaker regulation.[94] For example, if data is entered into a global database in China and is available in the twenty offices in which the service supplier has offices, such a scenario will prove highly complicated when it comes to untangling jurisdictional issues.[95]

Concurrent legislative jurisdiction, with multiple states having privacy laws governing a situation, has resulted in legal uncertainty. To date, various approaches have evolved to settle situations in which a conflict of laws exists.[96] Legislative

---

Data, 125 Yale L.J. 326, 236–251 (2015); Ned Schultheis, *Warrants in the Clouds: How Extraterritorial Application of the Stored Communications Act Threatens The United States' Cloud Storage Industry,* 9 Brook. J. Corp. Fin. & Com. L. 661, 668–683 (2015).

87 *See generally* Shin-yi Peng, *The Soft Law Approach to Regulatory Harmonization: Are We Trading Away Privacy for Economic Integration?*, in *A 'Liber Amicorum': Mitsuo Matsushita, A Critical Assessment of the International Economic Law and Governance*(Julien Chaisse et al. eds, Oxford University Press 2016).

88 For a summary, *see* Chander & Lê, *supra* n. 14, at 708–712.

89 *See* e.g. Miriam Wugmeister et al., *Global Solution for Cross-Border Data Transfers: Making the Case for Corporate Privacy Rules*, 38 Geo. J. Int'l L. 449, 449–450, 451 (2007); Paul De Hert et al., *Three Scenarios for International Governance of Data Privacy: Towards an International Data Privacy Organization, Preferably A UN Agency?*, 9 I/S: J. L. & Pol'y for Info. Soc'y 271, 275 (2013).

90 Albright Stonebridge Group, *supra* n. 10.

91 *See also* Dennis D Hirsch, *In Search of the Holy Grail: Achieving Global Privacy Rules Through Sector-Based Codes of Conduct*, 74(6) Ohio St. L.J. 1029, 1036 (2013); *Interoperability: Analyzing the Current Trends & Developments*, Data Protection Law & Policy, http://www.e-comlaw.com/data-protection-law-and-policy/ (accessed 17 Sept. 2016).

92 *Id*.

93 *Id., See also* Wugmeister et al., *supra* n. 89.

94 Sunni Yuen, *Exporting Trust with Data: Audited Self-Regulation as a Solution to Cross-Border Data Transfer Protection Concerns in the Offshore Outsourcing Industry*, 9 Colum. Sci. & Tech. L. Rev. 41, 45 (2008); Damon C. Andrews et al., *Personal Jurisdiction and Choice of Law in the Cloud*, 73 Md. L. Rev. 313, 315 (2013).

95 *See generally* Christopher Yoo et al., *Regulating the Cloud* 135–164 (The MIT Press 2015); Christopher Yoo, *The Changing Patterns of Internet Usage*, 63 Fed. Comm. L.J. 67 (2010); Peng, *supra* n. 87.

96 *See* Determann et al., *supra* n. 57.

jurisdiction over data can be based on the nationality of the Internet user, the location of Internet service suppliers, or the location of data.[97] Among various norms, asserting legislative jurisdiction over data based on the location of the data appears to be a straightforward proposition and has been increasingly pursued by governments.[98] This explains the key rationale behind DR requirements: if the data centre is located in China, then Chinese law and regulations apply. In this context, arguments could be made that there is a genuine relationship between the ends, i.e. privacy protection, and the means, i.e. the DR measures.[99] The responding party invoking the DL exception in a potential dispute may successfully argue that the DR measures at issue, especially Types II and III, fall under the scope of the TPP's DL exception.

3.2[b] *Search and Seizure – Law Enforcement*

In addition to privacy protection, one recurring theme in favour of enhanced DR requirements is law enforcement. Recently, Microsoft won a landmark legal action against the U.S. government over the protection of data on non-U.S. servers.[100] The case centred on a search warrant issued by U.S. federal law enforcement officials in December 2013 requiring Microsoft to disclose emails for a particular msn.com email address that was related to a narcotics investigation.[101] The actual emails and their content, however, were stored overseas in Dublin, Ireland.[102] The U.S. government argued that since Microsoft is a US company and can easily obtain a copy of the data in the US, a US warrant would suffice.[103] In other words, there was no actual extraterritorial application of the search warrant, simply

---

97 Rebecca Eubank, *Hazy Jurisdiction: Challenges of Applying the Stored Communications Act to Information Stored in the Cloud*, 7 Geo. Mason J. Int'l Com. L. 161, 176–181 (2016).

98 *Id.,* at 181.

99 *Argentina – Financial Services*, *supra* n. 80, para. 7.684. The Appellate Body explained, in the context of Art. XX of the GATT, that a contribution exists when there is a genuine relationship of ends and means between the objective pursued and the measure at issue.

100 On 14 July 2016, the United States Court of Appeals for the Second Circuit ruled against the US Government in the case *Microsoft v. United States* (hereinafter the *Microsoft* case), stating that the government cannot compel Microsoft to turn over customer emails stored on servers outside the United States. http://pdfserver.amlaw.com/nlj/microsoft_ca2_20160714.pdf (accessed 10 Sept. 2016).

101 *In re Warrant to Search a Certain Email Account Controlled and Maintained by Microsoft Corporation* (hereinafter the *Microsoft* case – District Court) (2d Cir. 2015).

102 It is worth mentioning that Ireland has made itself an attractive site for digital technology companies to place their European headquarters. Among others, Microsoft and Facebook have used Ireland as a location to host data centres. Currently as much as 90% of Europeans personal data is processed by US services; 82% of Facebook's European data passes through Ireland. *See* Jonathan Stempely, *Microsoft Wins Landmark Appeal over Seizure of Foreign Emails*, Reuters News (14 July 2016), http://www.reuters.com/article/us-microsoft-usa-warrant-idUSKCN0ZU1RJ (accessed 10 Sept. 2016).

103 *Microsoft* case – District Court, *supra* n. 101, at 12.

because Microsoft could access the emails domestically.[104] Therefore, Microsoft must produce evidence or information to the court within its possession, custody, or control regardless of the location of that data.[105]

Microsoft tried to avoid compliance with the search warrant on the creative theory that the servers housing the email were located in Ireland. Microsoft continued to defend this position, arguing that extraterritorial application of the Stored Communications Act (SCA) violated international law and foreign policy.[106] Microsoft also argued that the proper avenue for the U.S. federal government to retrieve evidence located in Ireland is through the appropriate Mutual Legal Assistance Treaty (MLAT).[107] Microsoft contended that the U.S. federal government, by failing to request permission to obtain emails held within Irish borders, actually bypassed its MLAT obligation to Ireland in an attempt to obtain emails without going through the proper diplomatic channels.[108]

On 14 July 2016, the United States Court of Appeals for the Second Circuit concluded that the SCA does not authorize courts to issue and enforce against US-based service providers warrants for the seizure of customer email content stored exclusively on foreign servers.[109] The ruling is expected to have far-reaching implications for DR policies.[110] By recognizing that Microsoft's practical and jurisdictional limitation arguments have merit, the Second Circuit Appeals Court will likely fuel the development of DR regulations. Under Microsoft's position, law enforcement access to evidence is dependent upon the location of data.[111] Following the *Microsoft* case, governments may increasingly demand that telecommunications companies and Internet service providers store their citizens' data within their jurisdictions so as to avoid the reach of foreign law enforcement. Initiatives related to DR have gained momentum, and the Microsoft's victory will only reinforce DR measures around the world. After all, if government access to Internet information turns on the actual location of the data, it increases pressure for DR mandates and encourages governments to consider DR measures as a mechanism by which to ensure law enforcement access to electronic content.[112]

---

104 *Id*.

105 Schultheis, *supra* n. 86, at 661–670. Nora Ellingsen, *The Microsoft Ireland Case: A Brief Summary* (15 July 2016), https://www.lawfareblog.com/microsoft-ireland-case-brief-summary (10 Sept. 2016).

106 *Id*.

107 The *Microsoft* case, *supra* n. 100, at 41–42.

108 *Id*.

109 *Id.,* at 7–9.

110 *See* David R. Beneman et al., *Extraterritorial Search Warrants Rule Change*, 29-WTR Crim. Just. 9, 11 (2015); Frederick T. Davis, *A U.S. Prosecutor's Access to Data Stored Abroad – Are There Limits?*, 49 Int'l L. 1 19 (2015).

111 The *Microsoft* case, *supra* n. 100, at 7–9. *See also* Daskal, *supra* n. 86, at 327–328.

112 Albright Stonebridge Group, *supra* n. 10. *See generally* Reema Shah, *Law Enforcement and Data Privacy: A Forward-Looking Approach,* 125 Yale L.J. 543 (2015).

In the context of international economic order, the core of the issue is whether the MLAT process, as identified by the U.S. International Chamber of Commerce,[113] will prove an effective means to ensure that data is available to law enforcement personnel when they want it and will therefore constitute a 'less trade restrictive', 'reasonably available' alternative measure under the necessity analysis. When data is stored abroad, a domestic law enforcement agency must cooperate with its counterparts in relevant jurisdictions under the MLAT to gain access to the criminal data trail. However, the MLAT can be time-consuming, and there is no guarantee of access.[114] It is argued, for instance, that while the US hosts a myriad of data centres, American firms and the Department of Justice are frequently uncooperative participants in the MLAT process.[115] Worse, criminals may arguably fall outside the reach of law enforcement in cases in which an MLAT has not been secured between certain jurisdictions. This is why the Indian government has asked certain firms to move their servers in India in the aftermath of the 2008 Mumbai attack.[116] The same logic was also cited in Vietnam's Decree 72, as noted above.[117] Navigating the cumbersome MLAT process in order to conduct searches abroad is an inefficient and impractical method of obtaining overseas evidence in criminal investigations.

That being said, a TPP panel may once again borrow the jurisprudence of Article XX of the GATT to examine claims that the alternative measure is not reasonably available. In this regard, precedent holds that the weighing and balancing exercise under the necessity analysis contemplates a determination as to whether a WTO-consistent alternative measure is available, or whether a measure that is less inconsistent with the WTO is reasonably available.[118] In addition, as repeatedly stated by the Appellate Body, alternative measures must be WTO-consistent while providing an equivalent contribution to the achievement of the objective pursued through the challenged measure.[119] Citing *U.S. – Gasoline*, the

---

[113] Chander & Lê, *supra* n. 14, at 735. As Chander pointed out, currently the US has MLATs in force with fifty-six countries. US ICC has recognized the crucial role of MLATs in facilitating the lawful interception of cross-border data flow and stressed the need to focus on MLATs instead of localization measures.

[114] For the first half of 2013, for instance, Brazilian courts issued 237 orders requesting Google to hand over information. Google complied with only 46% of these requests, however. Courtney Giles, *Balancing the Breach: Data Privacy Laws in the Wake of the NSA Revelations*, 37 Hous. J. Int'l L. 543, 568 (2015).

[115] Hill, *supra* n. 33, at 26.

[116] Chander & Lê, *supra* n. 14, at 731.

[117] *Id*.

[118] *See* Panel Report, *European Communities – Measures Prohibiting the Importation and Marketing of Seal Products (EC – Seal)*, WT/DS400/R, 18 June 2014, paras 7.636–7.639. Appellate Body Report, *EC – Seal,* WT/DS400, paras 5.260–5.264.

[119] Appellate Body Report, *Id*., para. 5.261.

Appellate Body in *Brazil – Retreaded Tyres* confirmed that a proposed alternative must preserve 'for the responding Member its right to achieve its desired level of protection with respect to the objective pursued'.[120] This work argues that the responding party invoking a DL exception in a potential dispute will undoubtedly argue that MLAT cannot qualify as a 'genuine alternative', as the proposed measure must be not only less trade restrictive than the DR measures, but should also 'preserve for (the responding party's) right to achieve its desired level of protection' with respect to law enforcement or a criminal investigation.[121]

4 CONCLUDING REMARKS – CHALLENGES FOR THE TISA/TTIP NEGOTIATIONS

We raised the following questions at the outset of this article: Can the TPP Agreement help to reverse the trend of DR, and if so, how? In section 3, we indicated that the TPP's DL exception allows parties to maintain a DR measure in order to achieve a legitimate public policy objective as long as the measure can satisfy the necessity test. The 'ambiguity' of the DL exception will be clarified by TPP tribunals when a real dispute occurs. After examining the rationales of DR measures in the context of the necessity test, we find that the responding party invoking a DL exception will have strong arguments, especially when defending Types II and III of the DR measures.

What lessons can be learned from TPP's E-Commerce Chapter? The Deputy USTR has publicly acknowledged that the US proposal to establish broad rights for service suppliers to transfer data across borders is facing significant opposition in the ongoing TiSA and TTIP negotiations.[122] Additionally, the chief TiSA negotiator for the EU has argued strongly for the following: 'It is crystal clear that we are not going to negotiate anything that jeopardizes data protection in Europe. We are not going to enter into anything jeopardizing private data in TiSA.'[123] EU Justice Commissioner Viviane Reding has also repeatedly warned against the erosion of privacy during TTIP trade talks related to data protection issues, on the grounds that privacy is a 'fundamental right', and

---

[120] Appellate Body Reports, *China – Measures Related to the Exportation of Various Raw Materials* (*China – Raw Materials*), WT/DS394/AB/R / WT/DS395/AB/R / WT/DS398/AB/R, 22 Feb. 2012, para. 7.490.

[121] Schultheis, *supra* n. 86, at 678. In the *Microsoft* Case, the U.S. government repeatedly stressed that the MLAT process was an impractical method of obtaining the pertinent evidence in criminal investigations.

[122] Inside U.S. Trade, *Holleyman Says TISA Data Flow Proposal Faces Pushback, But Vows To Press On* (20 Feb. 2015).

[123] Inside U.S. Trade, *U.S. Tackles Restraints On Transfers Of Personal Data In TISA Proposal* (19 Dec. 2014).

as such, 'it is not negotiable'.[124] Based on the findings in section 3, we argue that with regard to TiSA and TTIP negotiations on e-commerce, the major challenge is the disciplinary fragmentation of global economic regulation. 'The science of law' is divided into separate disciplines, without much thought to interdisciplinary regulatory issues that are common to the entire systems of regulation.[125] As demonstrated by the controversy surrounding the DR, we are now facing an increasingly complex legal environment that requires a dynamic understanding of the interdisciplinary fragmentation between/among the IEL, conflict of laws, and criminal procedure law. We are therefore of the view that the DR issues in question confirm that IEL correlates to other areas of law. Future negotiations will require more collaborative interdisciplinary solutions, attained through productive dialogue with experts in private international law and criminal procedure law.

It is evident that the IEL alone cannot 'prevent the open Internet from breaking up into balkanized networks in which data flows are more frequently blocked', as advocated by the USTR.[126] In fact, the necessity test required under the DL exception creates intersections with other areas of law. The current focus on where the data is stored in the areas of both private international law and criminal procedure law, however, provides justification for DR measures under the IEL framework. There is clearly a growing need for laws pertaining to Internet jurisdiction, in both the legislative and enforcement realms, to change. Such change would allow for a more narrow interpretation of the DL exception – rendering it more difficult to satisfy the necessity test.

To conclude, when understood dynamically, the environment surrounding e-commerce has changed to the degree that paradigm shifts are required to keep up with the times.[127] Certain areas of law – specifically, private international law and due process models of criminal justice – are struggling to cope with these myriad complexities. With respect to legislative jurisdiction, the conflict of laws problem is unique in the area of the Internet. Concurrent jurisdiction, with multiple states having their own privacy laws governing a situation, has resulted in legal

---

[124] EU officials have stressed that privacy protection should not be on the TTIP E-commerce negotiating table. *See* Inside U.S. Trade, *Brussels Round Marks Re-Engagement On Market Access Offers In TTIP* (06 Feb. 2015). *See also* Ralf Bendrath, *Trading Away Privacy: TTIP, TiSA and European Data Protection* (19 Dec. 2014), http://www.eurozine.com/articles/2014-12-19-bendrath-en.html (accessed 17 Sept. 2016).

[125] Shin-yi Peng, *Emergency Safeguard Measures for Trade in Services: A Case Study of Intra-Disciplinary Fragmentation*, in *International Economic Law after the Crisis: A Tale of Fragmented Disciplines* 237, 261–262 (C.L. Lim et al. eds, Cambridge University Press 2015).

[126] USTR, *supra* n. 63.

[127] *See* Anne S.Y. Cheung &Rolf H. Weber, *Internet Governance and the Responsibility of ISPs*, 26 Wis. Int'l L.J. 403–477 (2008); Christopher Yoo, *Possible Paradigm Shifts in Broadband Policy*, 9 J. L. & Pol'y for Info. Soc'y 367, 368 (2014).

uncertainty. With respect to enforcement jurisdiction, the warrant regime should be modernized in order to keep pace with the extraterritorial nature of digital technology and the needs of governments.[128] As publicly stated by Microsoft's legal officer Brad Smith following Microsoft's victory over the U.S. government, the court's decision should 'bring an impetus for faster government action so that both privacy and law enforcement needs can advance', which 'requires both new domestic legislation and new international treaties'.[129] Indeed, true and substantial changes in the theories and practices of Internet jurisdiction would allow us to argue for a more narrow interpretation of Article 14.13(3)(b) of the TPP: the DL exception. Without meaningful interdisciplinary dialogue between key government and non-government stakeholders, key DR questions will remain largely unanswered.

[128] Westmoreland et al., *supra* n. 86, at 225.

[129] *Microsoft Wins Landmark Irish Data Slurp Warrant Case against the US* (14 July 2016), http://www.theregister.co.uk/2016/07/14/microsoft_wins_landmark_irish_warrant_case_against_usa/ (accessed 10 Sept. 2016).