CURRENT ISSUES OF CROSS-BORDER PERSONAL DATA PROTECTION IN THE CONTEXT OF CLOUD COMPUTING AND TRANS-PACIFIC PARTNERSHIP AGREEMENT: JOIN OR WITHDRAW

GEORGE YIJUN TIAN*

Cross-border data flows are now a fundamental component of commerce. This paper explores the implications of ever-improving digital technology (particularly cloud computing technology) and examines some major policy and legal challenges in relation to cross-border personal data protection, which governments, businesses, and individual consumers have to address in the context of cloud computing and the Trans-Pacific Partnership (TPP) agreement.

This paper first examines the recent development of cloud computing (CC) technology and personal data protection. It then focuses on three challenging areas for transnational personal data protection: privacy and security, jurisdiction, and convergence. It also examines the new requirements under the TPP on cross-border data flows and data localization and their implications on existing challenges and future privacy law reform. It contends, although TPP is the "first" international agreement establishing a link between privacy and trade, its impacts should be not overstated. Given the borderless nature of the Internet, in order to identify an effective solution, the relevant laws and policies in some major economies (including both TPP and non TPP countries), such as the United States, the European Union, China and Australia, are delineated and compared. Finally, in line with the recent debates on TPP withdrawal in the US and Australia, it attempts to explore both

* Dr George Yijun Tian is a Senior Lecturer of Faculty of Law at the University of Technology Sydney (UTS), and a UDRP Neutral appointed by World Intellectual Property Organization (WIPO) Arbitration and Mediation Center, Geneva. The author is grateful to Professor Jill McKeough, former Law Dean of UTS and Commissioner for Australian Law Reform Commission (ALRC)'s Inquiry into Copyright Law, for her valuable comments through the paper writing. The author also would like to thank Professor Peter Yu (Texas A&M University School of Law) and Professor Dan Svantesson (Bond University School of Law) for their valuable comments for the early draft of the paper. The author also would like to thank all WILJ editor(s), particularly Ms. Anna L Grilley, for providing many useful comments in relation to copy editing.

opportunities and risks of joining or withdrawing from the TPP, and provide some practical suggestions for future law reform.

INTRODUCTION: CLOUD COMPUTING V. UNPREDICTABILITY OF DATA FLOWS

The Internet is relentlessly affecting all of our institutions, forms of communication, and social habits.[1] Increases in speed and bandwidth now make Cloud Computing (CC) a significant new player in the way information is collected, stored, handled, and distributed by individuals, business, and government agencies.[2] This not only profoundly impacts cross-border personal data transfer and protection, but also all information-related international trade.

The significance of CC and cross-border personal data protection to international trade has been reorganized by most major economies and has become an integral part of many regional trade agreements, including the Trans-Pacific Partnership (TPP) agreement and Free Trade Agreements (FTAs). Like many FTAs, TPP contains a special chapter on E-Commerce and cross-border personal data flows, which imposes extra

---

1 Christina Spiesel, *Eyes on the Horizon*, 58 MCGILL L.J. 1061, 1061 (2013).

2 PETER MELL & TIMOTHY GRANCE, NAT'L INST. OF STANDARDS AND TECH., THE NIST DEFINITION OF CLOUD COMPUTING: RECOMMENDATIONS OF THE NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY 2 (SPECIAL PUBLICATION 800-145, 2011).

obligations for members to follow.[3] In recent times, a *new tendency* has become apparent—as an increasing number of countries are reconsidering their involvement in existing multilateral trade arrangements, including the TPP and FTAs.[4]

This paper aims to examine the current issues related to cross-border personal data protection in the context of Cloud Computing and the Trans-Pacific Partnership Agreement. In line with the recent debates on the possible withdrawal of the United States and Australia from the TPP, both the opportunities and risks of joining in or withdrawing from the TPP will be identified alongside some practical solutions for regulators in different national contexts.

More specifically, first, this paper examines the recent development of Cloud Computin technology and personal data protection. It then focuses on three challenging areas for transitional personal data protection. Namely, the issues associated with privacy and security, jurisdiction, and convergence. It then examines the new requirements under the TPP on cross-border data flows and data localization and its implications on existing challenges and future privacy law reform. It contends, although the TPP is the "first" international agreement establishing a link between privacy and trade, its impacts should not be overstated. Given the borderless nature of the Internet, in order to identify an effective solution, the relevant laws and policies in some major economies (including both TPP signatories and non TPP signatory countries), such as the United States, the European Union, China, and Australia, are examined and compared. Finally, in line with the recent debates on the TPP withdrawal in the United States and Australia, it attempts to explore both opportunities and risks of joining in or withdrawing from the TPP. Specifically, it argues that prospective signatories must undertake a carefully considered cost-benefit analysis before entering into the TPP. Finally, some practical suggestions are provided for future law reform drawing on insights from the TPP.

---

[3] *Trans-Pacific Partnership Agreement*, AUSTL. GOV'T DEP'T OF FOREIGN AFF. & TRADE ch. 14 (Oct. 6, 2015), http://dfat.gov.au/trade/agreements/tpp/official-documents/Pages/official-documents.aspx [hereinafter TPP].

[4] Graham Greenleaf, *The TPP & Other Free Trade Agreements: Faustian Bargains for Privacy?* (UNSW Law Research Paper No. 2016-08, Feb. 14, 2016) (providing many specific examples in relation to this type of FTAs).

I. CLOUD COMPUTING & TRANSNATIONAL NATURE

Before examining the in-depth impacts, it is necessary to understand the key feature of CC technology. What is Cloud Computing? Generally speaking, CC is a relatively new business model in the information communication technology (ICT) industry. Scientists, law professors, and journalists often provide differing definitions of CC.[5] Indeed, after years of deliberation and 15 drafts, the U.S. National Institute of Standards and Technology's (NIST) arrived at the following definition for Cloud Computing in 2011.[6] The *NIST Definition of Cloud Computing* states, "cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction."[7] Alternatively, in 2013 Harvard University Law Professor Urs Gasser and David R. O'Brien defined CC as, "an umbrella term for an emerging trend in which many aspects of computing, such as information processing, collection, storage, and analysis, have transitioned from localized systems (i.e., personal computers and workstations) to shared, remote systems (i.e., servers and infrastructure accessed through the Internet.)"[8] Xath Cruz, an online editor of *Cloud Times,* defined CC more simply, as "any type of computing that can be done remotely through the Internet instead of locally."[9] Indeed, it is not an easy task to provide a strict and standardized definition of CC since there are different variations and technologies involved, and CC itself is an evolving technology.

In comparison with traditional Internet technology, one of the major improvements of CC is that computational resources under CC

---

[5] *See* Steven Rosenbush, *The Morning Download: Cloud Computing Hazy Meaning Creates Confusion for CIO's*, WALL ST. J. (Oct. 8, 2016), http://blogs.wsj.com/cio/2016/10/18/themorningdownloadcloudcomputingshazymeaningcreatesconfusionforcios/; *Defining Cloud Computing*, N.Z. L. SOC'Y (July 4, 2014), https://www.lawsociety.org.nz/lawtalk/lawtalk-archives/issue-845/defining-cloud-computing; Lizhe Wang, Jie Tao, & Marcel Kunze, *Scientific Cloud Computing: Early Definition and Experience*, IEEE COMPUTER SOCIETY (2008).

[6] *See* MELL & GRANCE, *supra* note 2, at 2.

[7] *Id.*

[8] DAVID R. O'BRIEN & URS GASSER, *Cloud Computing and the Roles of Governments*, *in* INTERNET MONITOR 2013: REFLECTIONS ON THE DIGITAL WORLD 25, 25 (Urs Gasser, Robert Faris & Rebekah Heacock eds., 2013).

[9] Xath Cruz, *Cloud Computing and its Legal Implications*, CLOUD TIMES (Dec. 3, 2012), http://cloudtimes.org/2012/12/03/cloud-computing-and-its-legal-implications/.

technology are elastic and can be shared by many simultaneous remote users and can be scaled up or down with demand.[10] This may significantly reduce the operational costs and increase the ease of service providers and users. For example, private clouds can be scaled to meet client's changing IT system demands. Public users can store their MP3 music, video, photos, and documents online instead of personal computers at home. This gives users the freedom to access their documents wherever they can find the means to access the Internet. This major improvement offers substantial business opportunities, but also initiates many potential legal challenges for personal data protection, particularly cross-border personal data protection.

A key feature of CC technology is that it is transnational in nature. CC technology permits data transmissions that span the globe. Data processing activities shift from country-to-country depending on load capacity, time of day, and a variety of other factors. These decisions are sometimes "made in real time and by machines rather than human."[11] As such, cloud users—even cloud providers—may not be able to know the true location of physical infrastructure as well as the true location of personal data. Although traditional Internet technology allows cross-border data transactions, in these transactions, data owners and processors seem to have better control over the data they process. At least, they know where the data is stored (location of database infrastructure) and where the data will be sent to (destination of data). As such, CC has arguably increased the "unpredictability" of data control and the uncertainty of legal compliance.

This is particularly pertinent in the current international trade environment. A company, either operating internationally or dealing with international clients, has to comply with the laws in relevant countries. If the company uses a cloud service provided by any third party, the provider is required to ensure compliance with the relevant laws of the country in question. For example, if an Australian company has entered into an agreement with a cloud provider in the United States, but the cloud provider hosts the data on a server in the EU, this means that the company needs to comply with laws in Australia, the U.S., and the EU. It also means that the company needs to guarantee that its cloud service

---

[10] NIKOLAS ROMAN HERBST, SAMUEL KOUNEV & RALF REUSSNER, ELASTICITY IN CLOUD COMPUTING: WHAT IT IS, AND WHAT IT IS NOT (2013).

[11] Paul M. Schwartz, *EU Privacy and the Cloud: Consent and Jurisdiction Under the Proposed Regulation*, 12 BNA PRIVACY AND SECURITY L. REP. 718, 718 (2013).

provider complies with the laws (such as privacy law) in all three different jurisdictions.

II. MAJOR CHALLENGES IN RELATION TO CROSS-BORDER PERSONAL DATA PROTECTION

Before examining the potential impacts of the TPP on cross-border personal data flows and Electronic Commerce (EC), it is necessary to examine the traditional legal challenges CC instigates about personal data protection, particularly cross-border personal data protection. Among all potential legal challenges, both CC service providers and users should take particular note of three major challenges: (1) jurisdiction; (2) privacy and security; and (3) convergence.

A. THE JURISDICTIONAL CHALLENGE

Many cloud providers are based overseas, particularly low-cost high-volume providers of applications. For example, if a customer in China signs a cloud service contract containing a "jurisdiction clause" which refers to Californian law, it is likely that the customer will refrain from enforcing their contract overseas due to financial limitations.

As businesses move towards using cloud services, data location becomes increasingly important. Subsequently, the clauses in relation to location of data perform an important role in determining the jurisdiction, as well as the level of data and privacy protection cloud users are afforded. For example, data protection in developed countries (such as the U.S. and Australia) may be markedly different from that of developing countries (such as China and India).[12] The United States introduced its *Privacy Act* in 1974.[13] In contrast, China's *Personal Information Protection Law* is still in the drafting process.[14]

---

[12] China does not have a formal Privacy Act yet. It is still in the drafting process. For more details, please see another paper of mine: Graham Greenleaf and George Tian, *Data Protection Widened by China's Consumer Law Changes*, 126 PRIVACY L. & BUS. INT'L REP. 127, (Dec. 2013).

[13] See The Privacy Act of 1974, 5 U.S.C. § 552a (2014), which "establishes a code of fair information practices that governs the collection, maintenance, use, and dissemination of information about individuals that is maintained in systems of records by federal agencies." *Privacy Act of 1974*, DEP'T OF JUST., https://www.justice.gov/opcl/privacy-act-1974 (last updated July 17, 2015).

[14] *See* PAUL DE HERT AND VAGELIS PAPAKONSTANTINOU, THE DATA PROTECTION REGIME IN CHINA 23 (2015).

Traditionally, it is relatively easy to find the location of web servers, and data is usually stored in the data centers of web service providers. In a cloud environment, many cloud providers are using virtual servers to provide data storage and process services. It is not always easy to identify where the data is actually located. As introduced above, in many circumstances, even cloud service providers may not know the true location of data storage.[15]

In addition, both the primary location of the data and any backup locations determine which countries' laws and regulations must be followed. Some large cloud service providers have data centers in different countries. Amazon Ltd. Co. for example has its data centers in California, USA, but it also has its backup data centers in many other places, including London and Tokyo.[16] The cost burden on the user to pursue legal proceedings or enforce the contract compounded by the lack of information available and the various political contexts involved increases the complexity of jurisdiction determination. For example, if Japan has been determined to have a jurisdiction (assuming the data breach was found in the data center located in Tokyo), the cost burden on the user to pursue legal proceedings in Japan would arguably be higher since many evidential documents need to be translated into Japanese. Thus, it is important to make sure that the locations of all relevant data centers have been fully disclosed under SLAs so that the parties can anticipate potential legal risks.

1. Jurisdiction Clauses & Data Location Clauses under Service Level Agreements (SLAs)

In cloud-computing related disputes, jurisdictional issues are always complex. Many potential jurisdictional challenges have been generated or intensified through cloud service contracts.[17] Jurisdiction clauses in cloud service contracts specify the applicable law governing the contract. For example, an American provider with a data center in Singapore can stipulate that a contract with an Australian customer is subject to Singaporean law, while contracts with American citizens are

---

[15] Schwartz, *supra* note 11.

[16] *See AWS Global Infrastructure*, AMAZON WEB SERVS., https://aws.amazon.com/about-aws/global-infrastructure (last visited Feb. 28, 2015) (providing a map of Amazon's global infrastructure).

[17] *E.g.*, TPP, *supra* note 3.

governed by the laws of the United States.[18] Contracts that contain jurisdiction clauses that direct the applicable law away from where the user is domiciled may result in a limited capacity to enforce the contract. Accordingly, both cloud providers and users need to be attentive to Service Level Agreements (SLAs). Indeed, cloud providers and users need to pay particular attention to the "jurisdiction clause" and the "data location clause" under SLAs. [19]

2. Service Level Agreements v. Access by Governments

A good SLA alone, even one with a proper "jurisdiction clause," does not mean that cloud users and providers are free from all potential jurisdictional challenges. When a cloud service provider has data centers in various countries, in addition to data breach and abuse by an individual or any third-party overseas, there is a risk of data breach by governments, by both domestic and foreign governments.[20] In addition, governments often have "dual roles" in relation to access to personal data in the cloud—either as regulators or as cloud service users.[21]

Governments in many countries have regulations to compel cloud service providers to provide governments' access to personal data in certain circumstances, such as national security or law enforcement.[22] In such circumstances, it is always difficult for cloud service providers to refuse. Whilst some Internet service providers may object, many feel compelled to provide government access to their customers' personal data, should the request be made.[23] A typical example is the United States Government's *Patriot Act.* Many recent reports and press articles have

---

[18] MARK VINCENT, NICK HART & KATE MORTON, TRUMAN HOYLE, CLOUD COMPUTING CONTRACTS WHITE PAPER: A SURVEY OF TERMS AND CONDITIONS (Apr. 5, 2011).

[19] Sasha Segall, *Jurisdictional Challenges in the United States Government's Move to Cloud Computing Technology*, 23 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1105, 1109 (2013) (stating that "the location of data storage often has choice-of-law implications").

[20] *See, e.g.*, Alan Travis, *UK Security Agencies Unlawfully Collected Data for 17 Years, Court Rules*, THE GUARDIAN, Oct. 18, 2016; Robert McMillan & Jennifer Valentino-Devries, *Russian Hacks Show Cybersecurity Limits*, WALL ST. J., Nov. 1, 2016.

[21] *See, e.g.*, USA Patriot Act of 2001, 18 U.S.C. § 2511(2) (2006); ALLEN & OVERY, THE EU GENERAL DATA PROTECTION REGULATION (2016) http://www.allenovery.com/SiteCollectionDocuments/Radical%20changes%20to%20European%20data%20protection%20legislation.pdf.

[22] USA Patriot Act § 2511; Regulation of Investigatory Powers Act 2000, c. 23 (UK).

[23] Francoise Gilbert, *USA Patriot Act Effect on Cloud Computing Services*, IT LAW GROUP, http://www.itlawgroup.com/resources/articles/113-usa-patriot-act-effect-on-cloud-computing-services (last visited Mar. 13, 2016).

expressed concern and asserted, "The US government has the unfettered ability to obtain access to data stored outside the United States by US cloud service providers or their foreign subsidiaries."[24] There are also concerns that the *Patriot Act*, "Allows US law enforcement and national security agencies unrestricted access to any data, anywhere, anytime."[25]

Like the United States, other jurisdictions have comparable legislation to enable their government agencies to require access to personal information in the context of national security or law enforcement. For example, in addition to the Chinese *Counter-Terrorism Law* (introduced above), the Standing Committee of the National People's Congress approved the *National Security Law of China*, effective as of July 1 2015, which contains detailed requirements in relation to the governments' access to personal data.[26] Furthermore, the Chinese State Internet Information Office (SIIO) announced a draft of new procedures to assess potential security problems with Internet technology and services used by sectors relating to national security and the public interest.[27] The new procedures propose the establishment of an Internet security assessment regime for important Internet related products/services and their suppliers entering the Chinese marketplace.[28] In other words, the products and services, which do not comply with the relevant security requirements, arguably, will be excluded from use in China. This new legislation and the accompanying procedures may oblige technical companies to share sensitive data and technology, like encryption processes (as introduced above). Companies—such as Cisco Systems, IBM, and Microsoft—would be affected by the procedures. It seems that, through these new regulations, China is attempting to impose similar restrictions to those in the United States.

In summary, laws or procedures, which compel cloud service providers to allow governments' access to personal data, may be a major headache for companies that sell Internet hardware and services overseas, especially to governmental sectors. On the one hand, these

---

[24] *Id.*

[25] *Id.*; USA Patriot Act § 2511.

[26] National Security Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., July 1, 2015), art. 51.

[27] *See Procedural Regulations for Administrative Law Enforcement Concerning Internet Information Content Management (Opinion-Seeking Draft)*, art. 1 (Rogier Creemers, ed., Jan. 14, 2016), https://chinacopyrightandmedia.wordpress.com/2016/01/14/procedural-regulations-for-administrative-law-enforcement-concerning-internet-information-content-management-opinion-seeking-draft/.

[28] *Id.* at art. 5.

companies are obligated to protect their customers against inadequate data protection, as well as intrusive government surveillance practices.[29] On the other hand, they need to be aware of the potential risks of breaching local laws or policies relating to national security as they operate businesses overseas.

B. THE PRIVACY AND SECURITY CHALLENGE

Data security is a major concern for any business or individual considering moving to the Cloud. There are a number of privacy and security risks for personal data protection in the cloud, particularly cross-border data protection.

1. Cross-Country Data Transfer and Legal Compliance

Data on the Internet will be transferred across the world,[30] and therefore data owners, cloud service providers, and data users need to deal with the *privacy and security risks associated with cross-country data transition* and legal compliance issues in relation to cross-country data transition.[31]

Some countries have amended their domestic laws to address cross-country data transition. For example, in March 2014, Australia introduced a range of updated privacy laws and replaced the National Privacy Principles (NPPs) with the Australian Privacy Principles (the APPs).[32] The new APPs contain a special principle on cross-border disclosure of personal information. This principle requires, prior to the disclosure of personal information relating to an overseas recipient, that an APP entity takes reasonable steps to ensure that the Australian Privacy principles are not breached.[33] Similarly, the data protection laws

---

[29] Camille Blackburn, *New Technology, Personal Data Protection and Implications for Financial Services Regulations*, JASSA THE FINSIA J. OF APPLIED FIN. 62 (2015).

[30] *See also* Milton L. Mueller, *The Politics and Issues of Internet Governance*, INST. FOR RES. & DEBATE OF GOVERNANCE (2007), http://www.institut-gouvernance.org/en/analyse/fiche-analyse-265.html.

[31] Peter K. Yu, *Towards the Seamless Global Distribution of Cloud Content*, *in* PRIVACY AND LEGAL ISSUES IN CLOUD COMPUTING, 180–81 (Anne S.Y. Cheung & Rolf H. Weber, eds., 2015) (providing a discussion on "territoriality questions implicated by cloud computing").

[32] *Privacy Fact Sheet 17: Australian Privacy Principles*, AUSTL. GOV'T: OFF. OF THE AUSTL. INFO. COMM'R (Feb. 2013), https://www.oaic.gov.au/images/documents/privacy/privacy-resources/privacy-fact-sheets/privacy-fact-sheet-17-australian-privacy-principles_2.pdf.

[33] It explicitly provided that "before an APP entity discloses personal information about an individual to a person (the overseas recipient):. . . the entity must take such steps as are

of the European Union (EU) member states also have provisions that specifically limit the ways in which the transfer of personal data outside these regions need to be handled.[34] The European Data Protection Directive (the Directive) obligates all collectors of the data or data controllers to inform individuals when their data will be sent and processed outside of the EU, and obligates all the data controllers and processors to have contracts approved by the Data Protection Authority in advance.[35] Arguably, these laws have a direct impact on how personal information is stored and transferred effectively overseas.

Despite growing regulation in the ICT sector in Europe, the United States and Australia, as well as many other countries, such as China, have not yet enacted similar laws addressing cross-border data transfer issues. Unlike in the European Union and various other Asia-Pacific countries, there is no single law in China aiming exclusively at personal data protection or cross-country data transfer. In December 2012, the National People's Congress Standing Committee took steps toward strengthening electronic data protection by issuing its *Decision on Strengthening Online Information Protection*.[36] This decision does not extend to address the issues pertaining to transnational data transfer specifically.

The globalized nature of data transfer in contrast with the limitations of national law has created a patchwork system of laws that apply at the domestic level, although the storage and transfer of data is international. As such, when cloud service providers set up data storage centers, to avoid legal ramifications they need to be aware of and comply with the laws in the country in which their data storage centers are located, particularly the laws in relation to cross-border data transfer. Likewise, when cloud users choose their cloud service providers; they should be more informed of the location of their cloud service provider's

---

reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles . . . in relation to the information." *Id.*

[34] *See* Council Directive 95/46 arts. 26, 31 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, 1995 O.J. (L 281) 31 (EC).

[35] *Id.* The European Commission (EC) even provides *the Model Contracts for the transfer of personal data to third countries*. *The Model Contracts for the Transfer of Personal Data to Third Countries*, EUROPEAN COMM'N, http://ec.europa.eu/justice/data-protection/international-transfers/transfer/index_en.htm (last updated Nov. 24, 2016).

[36] *National People's Congress Standing Committee Decision Concerning Strengthening Network Information Protection* (Rogier Creemers, ed., Dec. 28, 2012), https://chinacopyrightandmedia.wordpress.com/2012/12/28/national-peoples-congress-standing-committee-decision-concerning-strengthening-network-information-protection/.

data storage infrastructure,[37] and the potential risk of their personal data being unprotected by the laws of the country where the user is based, which may result in a false expectation of privacy.

2. Cross-Country Outsourcing Arrangements

The *subcontracting and outsourcing arrangements* that involve foreign companies also present extra risks for both cloud service providers and users. These include: (1) risks for subcontractor businesses who must navigate with their relevant legal obligations in protecting personal data under foreign laws; and (2) privacy and security risks for the user who is perhaps unaware of the commercial or political arrangements relating to their personal data and the subsequent application of foreign laws.

Although the cloud provider market is expanding, there are still only a limited number of large companies that have the capacity to offer large-scale application and data hosting independently.[38] As a consequence, many small and medium companies may subcontract some or all of the hosting to another company, including companies in another country. When entering an agreement with a cloud service provider in the United States, users should not simply assume the data center is located in the United States and the *US Privacy Act of 1974* will be applied.[39] Rather, if the cloud service provider is subcontracting with another cloud service provider who has data centers overseas, such as in Ireland or China, the subcontractor arguably is also required to follow the laws in these countries (as discussed above). And this may place some unexpected risks for users. For example, in certain regions, laws may allow local government unlimited access to the data regardless of its sensitivity. Additionally, cloud service providers may even be limited (or prohibited) from encrypting the data without ensuring local authorities can decrypt it as needed.[40] For example, in December 2015, China's Congress passed the new "*Counter-Terrorism Law"* that requires

---

[37] This includes their primary and backup locations, as well as any intermediate locations if data is being transferred between jurisdictions.

[38] Apple has spent 5 billion dollars on creating cloud computing data storage centers. Likewise, Facebook has acquired a 430, 000 square feet warehouse for the purposes of storage, while Google has developed 'Googleplex' 'a collection of movable glass buildings that can expand or contract as business requires. Other major companies include Samsung and Uber. *See Why Giants Thrive*, THE ECONOMIST (Sept. 17, 2016).

[39] The Privacy Act of 1974, 5 U.S.C. §552a (1974).

[40] Investigatory Powers Bill 2016, c. 25 (UK).

technology companies to assist the government in decrypting content in certain circumstances.[41]

As such, when choosing cloud service providers, users should be aware of any subcontracting arrangements in order to understand not only who will deliver the service but also who legally has access to the data. Otherwise, this may incur unnecessary data security risks.

C. CONVERGENCE CHALLENGE

Convergence challenges for cross-border personal data protection are two-fold: (1) challenges from the convergence of technology; and (2) challenges from the convergence of laws.

1. Challenges from Convergence of Technology

As computing and IT become further embedded into our daily activities and relationships, IT provides "not only a technology but also a core thing to integrate and converge with several other industry technologies, causing new industries, products and services."[42] Blackman[43] uses "digital convergence" to explain the evolution of technology services and industry, however the term has been further developed by Collins[44] and Gates[45] to describe the "coming together of telecommunications, computing and broadcasting into a single digital bit stream." [46] Digital convergence presents both opportunities and risks; it has significantly promoted innovation, efficiency, and contributed to public enjoyment of new technology. It also poses challenges, however,

---

[41] Counter-Terrorism Law of the People's Republic of China (promulgated by the Standing Comm. Nat'l People's Cong., Dec. 27, 2015), art. 18.

[42] *Digital Convergence and Interface for Cloud Computing Era*, DEPENDABLE COMPUTING LAB, http://dclab.yonsei.ac.kr/research/digital-convergence-and-interface-for-cloud-computing-era/ (last visited Feb 18, 2017).

[43] Colin R. Blackman, *Convergence between Telecommunications and Other Media: How Should Regulation Adapt?*, 22 TELECOMM. POL'Y 163, 164–65 (1998).

[44] Richard Collins, *Back To The Future: Digital Television and Convergence in the United Kingdom*, 22 TELECOMM. POL'Y 383, 385 (1998).

[45] Arlan Gates, *Convergence and Competition: Technological Change, Industry Concentration, and Competition Policy in the Telecommunications Sector*, 58 U. OF TORONTO FAC. OF L. REV. 83 (2000).

[46] Martha Garcia-Murillo & Ian Macinnes, *The Impact of Technological Convergence on the Regulation of ICT Industries*, 5 INT'L J. ON MEDIA MGMT. 57, 57 (2002).

for traditional models of commercializing and protecting personal information (personal data), including cross-border personal data.[47]

A recent example highlighting these challenges is the new mobile application being promoted by insurance giant AAMI.[48] The application aims to record and reward safe driving and discourage illegal driving behavior, such as texting, phoning, and speeding.[49] Not publicized is the possibility that the Safe Driver App may not only allow AAMI to increase insurance premiums based on a driver's score, but also enable AAMI to hand over data to police without notifying application users.[50] As discussed above, AAMI, as a company is legally able to disclose and share its customers' personal information with any third party, including law enforcement agencies and in doing so, possibly provide incriminating evidence against their customers. Accordingly, this app has instigated an intense debate on the legality of this new business model.[51]

2. Challenges from Convergence of Law

Like many other new cloud business models, the AAMI app may result in potential disputes across various areas of law (such as privacy, road safety, competition, and consumer protection laws) rather than a dispute being contained solely within insurance law.[52] It is clear that the "convergence of technology" has intensified the "*convergence of law" across different law sectors.* The Internet is borderless in nature. When goods or service providers put their products or services (including intangible products, such as gaming software) on the Internet, they are

---

[47] Paul T. Jaeger et al., *Where is the Cloud? Geography, Economics, Environment, and Jurisdiction in Cloud Computing*, 14 FIRST MONDAY, (May 4 2009), http://firstmonday.org/ojs/index.php/fm/article/view/2456/2171 (Cloud computing "places enormous capacity and power in the hand of users. As an emerging new technology, however, cloud computing also raises significant questions about resources, economics, politics, the environment, and the laws").

[48] *See* Margot O'Neill, *Data Retention: AAMI Safe Driver App Could See Information Handed to Police, Premiums Go Up*, ABC NEWS (Mar. 10, 2015), http://www.abc.net.au/news/2015-03-10/aami-safe-driver-app-data-retention/6292198.

[49] *Id.*

[50] *Id.*

[51] *Id.*

[52] *Id.* The AAMI app aims to record and reward safe driving, and to discourage illegal driving behaviour, including texting, phoning and speeding (road safety law). But it may also enable AAMI to hand over data to police from its Safe Driver App without the consent from app users (privacy law) and to increase insurance premiums based on a driver's score (insurance, and competition and consumer law).

trading with customers worldwide rather than a single national market. As a consequence, the laws in foreign countries may extend the jurisdictions they are subject to.

For example, in another recent case in Australia, the Australian Competition and Consumer Commission (ACCC) sued a US software publisher, Valve Software, in the Australian Federal Court on the grounds that Valve's refund policies and subscriber agreements for its "Steam" platform (cloud platform) have breached the *Australian Consumer Law* (ACL).[53] Valve Corporation is a company incorporated in the United States. Its online computer game distribution platform (known as "Steam") has over 125 million users worldwide.[54] Valve does not have physical retail stores in Australia, but it has approximately 2.2 million users in Australia.[55]

Valve Corporation does not admit that it operated business in Australia, although it admits that it has made available to Australian consumers, online access to use video games through Steam Client pursuant to the terms of a Steam Subscriber Agreement (SSA).[56] Valve further claims the SSA was made under the law of the State of Washington in the United States and is not a contract to which the Australian consumer law applies.[57] In March 2016, the Australian court made a decision in favor of the ACCC. Justice Edelman concluded that, in any event, Valve was carrying on business in Australia and therefore Australian consumer law should apply.[58] Following this reasoning, when any Australian companies provide online gaming services to United States users or users in other countries, the consumer laws in these countries could arguably apply to the Australian companies. In summary, the increasing complexity of legal issues compounded by the multiplicity of jurisdictions to which companies are subject creates a legal terrain that is difficult for cloud computing providers to navigate.

---

[53] *Australian Competition & Consumer Comm'n v Valve Corp. [No. 3]*, 2016 FCA 196 (Austl.).

[54] Luke Plunkett, *There Are Over 125 Million "Active" Steam Accounts.*, KOTAKU (Feb. 24, 2015, 7:00 p.m.), http://kotaku.com/there-are-over-125-million-steam-accounts-1687820875.

[55] Press Release, Austl. Competition and Consumer Comm'n, Federal Court Finds Valve Made Misleading Representations About Consumer Guarantees (Mar. 29, 2016).

[56] *Australian Competition & Consumer Comm'n v Valve Corp. [No. 3]*, 2016 FCA 196, 1–2 (Austl.).

[57] *Id.* (The Court found that Valve made the following false or misleading representations to consumers, in the terms and conditions contained in three versions of its Steam Subscriber Agreement and two versions of its Steam Refund Policy).

[58] *Id.* at 34.

D. SUMMARY AND REMARKS: OVERLAPS AND INTERACTIONS

It is important to emphasize that any cloud service providers, users, and regulators, particularly for those who have to deal with cross-country personal data transactions, need to carefully consider the three major challenges introduced above: (1) privacy and security; (2) jurisdiction; and (3) convergence. These three challenges are deeply interlinked, and certain overlaps may exist among the three. The overlaps and interactions between the three challenges provide evidence for and reflect upon the nature of integration and convergence in the information technology industry ("convergence challenge").

III. RISE OF DATA LOCALIZATION MEASURE V. NEW REQUIREMENTS UNDER TRANS-PACIFIC PARTNERSHIP (TPP) AGREEMENT

A. RISE OF DATE LOCALIZATION MEASURES & THE RATIONALE BEHIND THE MEASURES

In response to the growing number of legal challenges brought by CC, an increasing number of countries have introduced measures to control personal data flowing across their borders.[59] Although the measures they adopted vary widely in both scope and intensity, a less contentious regulation that many countries adopt is a "data localization" measure.[60] Put simply, a data localization measure refers to any regulations or policies, which require companies to store and process data in data centers located physically within the national border.[61] Many countries have included "data localization" requirements into their legal frameworks in order to strengthen their controls of personal data flowing across their borders. These countries include TPP members, such as Vietnam, Malaysia, Australia (localization requirements for health records), and Canada (localization requirements for government data). In

---

[59] ALBRIGHT STONEBRIDGE GROUP, DATA LOCALIZATION: A CHALLENGE TO GLOBAL COMMERCE 1, 6 (September 2015) (For example, "In Brussels, officials have justified data localization as part of broader efforts by the European Union and national governments to regain control of information owned by U.S. multinational companies and subject to the prying eyes of the U.S. government.").

[60] Neha Mishra, *Data Localization Laws in a Digital World: Data Protection or Data Protectionism?*, THE PUBLIC SPHERE 137, 137 (2016) ("Data localization policies are proliferating across both liberal/democratic states such as Australia, Canada, and India, as well as illiberal states such as China, Vietnam,. . . Iran [and] Russia.").

[61] ALBRIGHT STONEBRIDGE GROUP, *supra* note 59, at 3.

addition to non-TPP members, such as the European Union, Russia, and China, which are major trade partners to most TPP members.[62]

Although the details, motivations, and scope of these measures are unique to each country, the rationales behind these measures are generally three-fold: first, to reduce the "unpredictability" of data control and the uncertainty of law compliance brought by CC technology (as discussed above–technical reasons); second, and more importantly, to strengthen their data control ability in order to improve their international competitiveness in the global information economy; third, to address national security concerns through increased access and control of data that identifies potential threats.

For example, EU officials in Brussels have justified data localization as part of broader efforts by the European Union and EU member governments to "regain control of information owned by U.S. multinational companies and subject to the prying eyes of the U.S. government."[63] Regarding the global information economy, in 2015, Gunther Oettinger, the EU Commissioner for the Digital Economy, explicitly expressed the EU's desire to wrest control of information from foreign entities, stating that, "the Americans are in the lead, they've got the data, the business models and so the power," and the European Union needs "stronger data-privacy safeguards to counter Google, Facebook, Apple and other U.S. companies offering Internet services and applications."[64] In addition, political and national security justify the reason for data localization requirements. As Geist summarized, data localization requirements "typically stem from mounting concerns over U.S. surveillance activities and the power granted to U.S. law enforcement under laws such as the *USA Patriot Act.*"[65]

By contrast, US commentators criticize complex compliance requirements in the EU, driven by recent court decisions and potential new regulations (e.g. the EU's *General Data Protection Regulation*

---

[62] *Id. See also Data Localization Snapshot*, INFO. TECH. INDUSTRY COUNCIL, https://www.itic.org/public-policy/SnapshotofDataLocalizationMeasures7-8-2016.pdf (last updated July 8, 2016).

[63] ALBRIGHT STONEBRIDGE GROUP, *supra* note 59, at 6.

[64] Tom Fairless, *Europe's Digital Czar Slams Google, Facebook*, THE WALL STREET JOURNAL (Feb. 24, 2015, 9:54 AM), http://www.wsj.com/articles/europes-digital-czar-slams-google-facebook-over-selling-personal-data-1424789664.

[65] Michael Geist, *How the TPP Puts Canadian Privacy at Risk*, HUFFINGTON POST (Oct. 14, 2015, 5:53 PM), http://www.huffingtonpost.ca/michael-geist/tpp-canadian-privacy_b_8296146.html.

(GDPR)),[66] which make an increasing number of foreign companies believe that in order to access the EU market, they "have no choice but to relocate server infrastructure in Europe."[67] In November 2015, Robert D. Atkinson, the President of the Information Technology and Innovation Fund, in his testimony before the House Judiciary Committee, stated that data flow restrictions imposed by other countries will harm the U.S. economy in at least two ways:

> First, requiring localization of data and servers will move activity from the United States to these nations, reducing jobs and investment here and raising costs for U.S. firms.
>
> Second, if the restrictions preclude U.S. firms from participating in foreign markets, then U.S. firms will lose global market share to competitors that are based in those protected markets.[68]

Although it seems that the spread of data localization has become a "global trend" and an increasingly popular legal method for strengthening the control and protection of personal information by both TPP and non-TPP countries (as mentioned above), such a trend may not be sustainable (at least to TPP members) due to the conclusion of the TPP Agreement negotiations led by the United States.[69] Although it may not be the first trade agreement that reflects privacy and personal data concerns, it is the first agreement to contain detailed provisions on privacy and explicitly obligate members to ban data localization laws and policies.

---

[66] Council Regulation 2016/679 of the European Parliament and the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data, and Repealing Directive 95/46/EC (General data Protection Regulation), (L 119) 1 (EC). On 8 April 2016 the Council adopted the Regulation and the Directive. And on 14 April 2016 the Regulation and the Directive were adopted by the European Parliament. On 4 May 2016, the official texts of the Regulation and the Directive have been published in the EU Official Journal in all the official languages. While the Regulation will enter into force on 24 May 2016, it shall apply from 25 May 2018. The Directive enters into force on 5 May 2016 and EU Member States have to transpose it into their national law by 6 May 2018.

[67] ALBRIGHT STONEBRIDGE GROUP, *supra* note 59, at 6.

[68] *Internet Data Flows: Promoting Digital Trade in the 21st Century Before the Subcomm. on Courts, Interllectual Prop. and the Internet of Justice of the H. Comm. on the Judiciary*, 114th Cong. 5 (2015) (statement of Robert D. Atkinson, Founder and President, The Information Technology and Innovation Foundation).

[69] Juro Osawa & Eva Dou, *China's Top Web Browsers Leave User Data Vulnerable, Group Says*, WALL ST. J. (Mar. 28, 2016, 5:00 PM), https://www.wsj.com/articles/chinas-top-web-browsers-leave-user-data-vulnerable-group-says-1459198802 (quoting Manuel Maisog).

B. NEW REQUIREMENTS UNDER THE TRANS-PACIFIC PARTNERSHIP AGREEMENT

After more than five years of negotiation, the TPP finally reached a successful conclusion on October 6, 2015.[70] The TPP negotiations were undertaken by twelve countries from both sides of the Pacific (including Australia, Brunei, Canada, Chile, Japan, Malaysia, Mexico, Peru, New Zealand, Singapore, the United States, and Vietnam) that together represent 40 percent of the global GDP.[71]

The TPP is the largest regional free trade agreement to date.[72] Apart from reducing trade barriers and offering new market access and investment opportunities, the TPP contains a special chapter on Electronic Commerce ("e-commerce" chapter), which ensures that trade conducted electronically between TPP countries takes place efficiently and with appropriate consumer protections.[73] For the first time, it explicitly obligates the member countries to (1) protect personal data, together with a commitment to (2) the freedom of cross-border data, and (3) information flows.

1. Three obligations on personal data protection

a. Protection of Personal Information

As the bedrock provision on the personal data protection, Article 14.8 of the TPP explicitly requires each member state to set up a "legal framework" for providing sufficient protection of the "electronic commerce" users.[74] Since a "legal framework" is required, this is clearly an advance on the *APEC Privacy Framework* (2004), which is not legally binding to its parties.[75] While recognizing that each member state may adopt different legal approaches to protect personal information, the TPP obligates member states to encourage the development of

---

[70] TPP, *supra* note 3.

[71] *Id.*

[72] *Id.*

[73] *Id.* at art. 14.7.

[74] *Id.* at art. 14.8(2).

[75] Asia-Pacific Economic Cooperation [APEC], *APEC Privacy Framework*, APEC Doc. No. 205-SO-01.2 (2005).

mechanisms or arrangements in order to "promote compatibility between various approaches."[76]

To increase compatibility, the TPP, for the first time, provides a clear and broad definition of "personal information," to mean, "any information, including data, about an identified or identifiable natural person."[77] This definition is a well-accepted approach to defining personal data and is similar to the position of major non-TPP economies, such as the European Union (EU). The new EU *General Data Protection Regulation* (GDPR) 2016 defines that "'personal data' means any information relating to an identified or identifiable natural person ('data subject')."[78]

All member states, with the exception of Brunei and Vietnam, which are in the process of implementing their respective "legal frameworks," have already established legal frameworks that provide for the protection of personal data.[79] As such, the TPP has taken an important step by attempting to enhance the harmonization of personal data protection rules and the enforcement of personal data protection rules in both TPP and non-TPP countries. It may still be too early, however, to conclude that the TPP has increased the level of personal data protection at the international level (more details will be discussed later).

b. Cross-Border Transfers of Personal Data (Prohibition on Data Export Limitations)

The TPP contains a provision, which specifically deals with cross-border data transfers by electronic means.[80] While recognizing that "each member state may have its own regulatory requirements concerning the transfer of information by electronic means," Article 14.11 obliges each member state to "allow the cross-border transfer of information by electronic means, including personal information, when

---

[76] TPP, *supra* note 3, at arts. 14.8.2 n.6, 14.8.5 (The TPP allows a member state to comply with the obligation under Art 14.8.2 "by adopting or maintaining measures such as a comprehensive privacy, personal information or personal data protection laws, sector-specific laws covering privacy, or laws that provide for the enforcement of voluntary undertakings by enterprises relating to privacy").

[77] *Id.* at art. 14.1 (Definitions).

[78] Council Regulation 2016/679, *supra* note 66.

[79] *See* TPP, *supra* note 3, at art 14.8 n.5 ("Brunei Darussalam and Viet Nam are not required to apply [Article 14.8] before the date on which that Party implements its legal framework that provides for the protection of personal data of the users of electronic commerce.").

[80] *Id.* at art. 14.11.

this activity is for the conduct of the business . . .'"[81] In comparison with the general protection provision under Art. 14.8, which only applies to the protection of the "users of electronic commerce" personal data, the scope of application of Art. 14.11 is much wider.[82] It covers all "cross-border transfer of information by electronic means."[83] Article 14.11 not only covers the transfer of commercial data (such as customers' credit card information), but also non-commercial data, such as the personal information of patients in a hospital or the personal information of employees in a company.[84]

The TPP also allows safe harbor (immunity) for member governments to impose conditions or restrictions on the "cross-border transfer of information" in certain circumstances.[85] More specifically, in order to obtain the immunity, such conditions or restrictions must satisfy four requirements:

> The measures "are required to achieve a legitimate public policy objective" (*public objective exemption*);[86]
>
> The measures are not applied in a manner that would "constitute a means of arbitrary or unjustifiable discrimination;"[87] or
>
> The measures are not applied in a manner that would "constitute a disguised restriction *on trade***;**"[88]
>
> The measures are *not* applied in a manner that would "impose restrictions on transfers of information *greater than* are required to achieve the objective."[89]

If a TPP member fails to meet any one of four requirements, the country's data export restrictions could face dispute settlement proceedings (more details will be discussed below). Additionally, the TPP leaves the onus on the member government imposing a restriction to prove its policy measure satisfies all four requirements.[90] Through these

---

[81] *Id.*

[82] *Id.* at art. 14.8.

[83] *Id.*

[84] *Id.* at art. 14.11.

[85] *Id.*

[86] *Id.* at art. 14.11.2.

[87] *Id.* at art. 14.11.3(a).

[88] *TPP Chapter Summary: Electronic Commerce*, AUSTL. GOV'T DEP'T OF FOREIGN AFF. & TRADE, http://dfat.gov.au/trade/agreements/tpp/summaries/Documents/electronic-commerce.PDF (last updated July 12, 2016); TPP, *supra* note 3, at art. 14.11.3(a).

[89] *Id.* at art. 14.11.3(b).

[90] Greenleaf, *supra* note 4, at 11–12.

provisions, for the first time, the TPP provides businesses with certainty about their ability to move data across borders.[91]

c. Freedom of data flows (Prohibition on data localization)

The TPP Agreement contains a prohibition provision on data localization.[92] Art. 14.13 (Location of Computing Facilities) explicitly prevents localization of "computer servers and storage devices for processing or storing information for commercial use," and obligates each member state not to implement any measures which require companies "to use or locate computing facilities in that [member state's] territory as a condition for conducting business in that territory."[93] In other words, any TPP member cannot impose requirements on a covered person to use or build a local data center (computing facilities) in order to conduct business in that TPP member's territory.

Nevertheless, in the same manner as the cross-border transfers of personal data provisions, the TPP still allows member states to introduce localization requirements for the purpose of achieving public policy objectives.[94] In order to justify the application of data localization measures, a member must prove that the localization measures satisfy four requirements: the measures are adopted or maintained "to achieve a legitimate public policy objective" (*public objective exemption*);[95] the measures are not applied in a manner that would "constitute a means of arbitrary or unjustifiable discrimination;"[96] or the measures are not applied in a manner that would "constitute a disguised restriction *on trade***;**"[97] the measures are *not* applied in a manner that would "impose restrictions on *the use or location of computing facilities greater than* are required to achieve the objective."[98]

---

[91] *Id.* at 12.

[92] TPP, *supra* note 3, at art. 14.13.

[93] *Id.* at art. 14.13.2.

[94] *Id.* at arts. 14.13.2, 14.13.3(a)–(b) (public objectives exemption).

[95] *Id.* at art. 14.13.3.

[96] *Id.* at art. 14.13.3(a).

[97] *TPP Chapter Summary: Electronic Commerce*, *supra* note 88; TPP, *supra* note 3, art. 14.13.3(a).

[98] *Id.* at art. 14.13.3. ("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 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."); *Id.* at art. 14.13.3(a).

Like the counterparts for data export limitation immunity, if a TPP member fails to meet any one of the four requirements, its data localization measures could face dispute settlement proceedings. Again, the TPP leaves the onus to member governments imposing data localization measures to prove its policy measures satisfy all four requirements.[99]

The introduction of the data localization prohibition provisions provide security to businesses that are making substantial investment decisions relating to the placement of data centers in TPP countries, and may significantly reduce market entry barriers between TPP countries.[100] It is not surprising that data localization measures are limited and can even be explicitly prohibited (subject to public objective exemption) by the TPP Agreement, since the TPP negotiation was initiated and oriented by the United States, which has suffered from the localization provisions of the EU personal data protection laws for a long time. It seems that the United States intends to use the TPP agreement to prevent future TPP members from making EU-style data localization legislation.

2. Dual Dispute Settlement Mechanisms

There are two sets of dispute settlement mechanisms under the TPP. First, it obligates the member countries to adopt an investor-state dispute settlement (ISDS) mechanism under Chapter 9 *Investment*.[101] It potentially applies whenever an investor from one member country makes an investment in the territory of the other member country.[102] ISDS enables an investor, who believes a TPP member government has breached its investment obligations, and whose attempts at resolution have failed, to take the matter to arbitration for possible compensation.[103] Arbitration would happen under rules administered by a respected international arbitration bodies selected by involved parties.[104] The TTP requires that the proceedings would be open and transparent,[105] and the

---

[99] Greenleaf, *supra* note 4, at 11.
[100] *Id.*
[101] TPP, *supra* note 3, at art. 9 (Investment).
[102] *Id.* at art. 9.2.
[103] *Id.* at art. 9.19.
[104] *Id.* at art. 19.19.5.
[105] *Id.* at art. 9.24.

arbitrators would be independent.[106] Second, the TPP contains a special chapter called *Dispute Settlement*.[107] Unlike ISDS, the Dispute Settlement Chapter governs disputes between governments of TPP members, rather than disputes between private parties and governments.[108] In case that all other attempts have failed, Chapter 28 allows all TPP members to have disputes resolved by arbitration.

The scope of the application of these two dispute settlement mechanisms are different. The ISDS mechanism applies exclusively to commitments in the investment chapter and relates to disputes between private parties and governments.[109] Article 9.6.3 of TPP explicitly elucidates, "[A] determination that there has been a breach of another provision of this Agreement, or of a separate international agreement, does not establish that there has been a breach of this Article."[110] Therefore, it seems that a breach by a member country of any provision that is not relevant to "investment" (e.g. the provisions in relation to personal data protection), will not automatically trigger the entitlement of affected companies to the ISDS provisions unless the affected companies can prove otherwise. By contrast, the dispute settlement mechanism (under Chapter 28) generally applies across the TPP Agreement, whenever one member considers that another member's "actual or proposed measure" does not comply with its obligations under the TPP.[111] So naturally, these procedures between states (under Chapter 28)

---

[106] *Id.* at art. 9.22. Most respected international arbitration bodies have an 'independence' requirement to select arbitrators. *See, e.g.*, Convention on the Settlement of Investment Disputes between States and Nationals of Other States, art. 14, Mar. 18, 1965, 575 U.N.T.S. 159; Int'l Centre for Settlement of Inv. Dispute [ICSID], *Rules Governing the Additional Facility for the Administration of Proceedings by the Secretariat of the International Centre for the Settlement of Investment Disputes*, art. 7, ICSID/11 (Apr. 2006), https://icsid.worldbank.org/en/Documents/icsiddocs/AFR_English-final.pdf (requiring arbitrators to be "persons of high moral character [with] recognized competence in the fields of law, commerce, industry or finance, who may be relied upon to exercise independent judgment."). *See also* G.A. Res. 68/109 Arbitration Rules of the United Nations Commission on International Trade Law, arts. 9–12 (Dec. 16, 2013) (requiring arbitrators to be impartial and independent , and to disclose anything likely to give rise to justifiable doubts as to the arbitrator's impartiality or independence). Arseni Matveev, *Investor-State Dispute Settlement: The Evolving Balance Between Investor Protection and State Sovereignty*, 40 U. OF W. AUSTL. L. REV. 348, 353 (2015).

[107] TPP, *supra* note 3, at ch. 28 (Dispute Settlement).

[108] *Id.*

[109] "A determination that there has been a breach of another provision of this Agreement, or of a separate international agreement, does not establish that there has been a breach of this Article." *Id.* at art. 9.6.3.

[110] *Id.*

[111] *Id.* at art. 28.7–.9.

will apply to any dispute concerning the Electronic Commerce provisions (including personal data protection provisions) under Article 14.[112]

C. NEW TENDENCY – WITHDRAWING FROM TPP

The increasing tendency of prospective or established member states to consider not proceeding with or even withdrawing from the TPP is noteworthy. In many countries, but particularly in the United States support for the TPP has waned for various reasons. In the United States, the TPP trade deal faced opposition from the 2016 presidential candidates in both major parties. Indeed, both Hillary Clinton and Donald Trump opposed the deal, arguing that it will hurt American workers.[113] Clinton contended she would only support the TPP trade deal as president if the agreement were revised in some way.[114] Going further, Trump promised withdrawal of the United States from the TPP.[115]

In Australia, the Coalition has been very active in negotiating free trade agreements, and the Labor Party has a policy of open trade.[116] But an increasing number of political parties or politicians have started to oppose the TPP. For example, Senator Nick Xenophon and his party (NXT) have been vocal in their criticism of the TPP and called for a more strategic and "hard-headed" approach to trade negotiations to protect Australian workers.[117] The Greens Party has been highly against the TPP for many years and has called for withdrawing from the TPP.[118] The Greens expressed strong concerns on the ISDS provisions. They

---

[112] *Id.* at art. 14.7.

[113] Stephen Greenhouse, *Hillary Clinton's TPP Deal Disapproval is 'A Critical Turning Point*, THE GUARDIAN, (Oct. 8, 2016).

[114] Eric Bradner, *Clinton's TPP Controversy: What You Need to Know*, CNN.COM (July 27, 2016) at http://edition.cnn.com/2016/07/27/politics/tpp-what-you-need-to-know/ (Clinton said she opposes the TPP because of its lack of a crackdown on currency manipulation and provisions to extend pharmaceutical drug companies' patent protections in poorer countries.).

[115] Jeremy Diamond, *Trump Slams Globalization, Promises to Upend Economic Status Quo*, CNN.COM (June 28, 2016, 20:51 GMT), http://edition.cnn.com/2016/06/28/politics/donald-trump-speech-pennsylvania-economy/.

[116] Paul Kiren et al., *The Free Trade Mythology of Added Prosperity*, THE AUSTL., (Aug. 24, 2016).

[117] Anna Vidot, *What Could Australia's More Trade-Sceptic Senate Mean for the Trans-Pacific Partnership?*, ABC RURAL (July 5, 2016) ("In response to being called a 'protectionist', Senator Xenophon said he would wear the description as a badge of honour for 'standing up for Australian manufacturing industry and the jobs of Australian workers'").

[118] Australian Greens Party, *Stop the TPP: The Biggest Trade Deal in our History is Far Worse Than Expected*, http://greens.org.au/campaigns/national/stop-tpp (last visited Nov. 12, 2016).

believe that the ISDS provisions, "will allow foreign investors to sue our government if their profits are affected by any Australian law or policy."[119]

It is clear that the vitality of the TPP regime is still questionable. Particularly, it is unclear whether existing TPP members will still proceed if the United States formally withdraws from the TPP. Member countries may stay or withdraw from the TPP for various reasons (not limited to privacy and e-commerce reasons). Next, this paper will examine potential impacts of the TPP on personal data protection, including both the opportunities and the risks of joining or withdrawing from the TPP.

IV. IMPLICATION OF PERSONAL DATA PROTECTION PROVISIONS OF THE TPP ON BUSINESSES

A. GENERAL IMPLICATIONS: THE LINK BETWEEN PRIVACY AND TRADE

Historically, privacy has not been an issue typically associated with trade agreements. While some former FTAs contain certain personal data related provisions, they mainly focus on freedom of data flows only.[120] It seems for the first time, however, that the TPP is attempting to establish a formal link between privacy and trade through very detailed provisions relating to personal data protection (under Chapter 14),[121] in a similar manner to the *Trade-Related Intellectual Property Agreements* (TRIPS Agreement)[122] under the World Trade Organization (WTO) framework.[123] More importantly, like the WTO, the TPP also contains dispute settlement mechanisms, under Chapter 9 Investment and Chapter 28 Dispute Settlement respectively.[124] Due to these dispute settlement mechanisms, it is likely that there will be an increase in the enforceability of privacy provisions under the TPP.[125] As the first

---

[119] *Id.*

[120] Greenleaf, *supra* note 4, at 3–7 (for specific examples, please see the section on "FTAs and privacy prior to 2015's TPP").

[121] *Id.* at 2.

[122] Agreement on Trade-Related Aspects of Intellectual Property Rights, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1C, 1869 U.N.T.S. 299 [hereinafter TRIPS].

[123] *Id.*

[124] TPP, *supra* note 3, at ch. 18 (Intellectual Property).

[125] This paper will not focus on the international dispute resolution mechanisms in relation to cross border data protection. The author will discuss this issue in a separate paper.

international trade agreement which contains both detailed privacy requirements and dual dispute settlement mechanisms, the TPP will have profound implications on future international privacy lawmaking (More details will be discussed in the recommendation section).

B. IMPLICATIONS OF PERSONAL DATA PROTECTION PROVISIONS UNDER TPP: OPPORTUNITY AND RISKS

The TPP data protection provision offers both substantial opportunities and risk.

1. Potential Opportunities

First, as mentioned above, data protection provisions under the TPP have arguably created the potential for member states to harmonize their personal data protection laws Asia Pacific-wide (APAC-wide). *Second*, the TPP helps reduce the cost of compliance with the law. As such, it reduces the cost of business operations across a "patchwork" of national data protection laws that regulate the collecting or processing personal data in member states, and the cross-border personal data transfers between member states.[126]

By adopting a more uniform approach and concerted effort towards the personal data protection, TPP will arguably help to build trust and confidence between businesses and consumers in TPP markets. More specifically, businesses will have the freedom and flexibility to store and process personal data across different TPP markets. For example, a large cloud service provider will be able to rely on economies of scale to serve multiple TPP markets using computing and data storage facilities (e.g. data centers) from fewer locations. They do not need to worry about the data localization rules of other member states, and do not need to build or invest in their data infrastructures in each TPP market that the business seeks to serve.[127]

---

[126] TPP, *supra* note 3, at art. 14.11. *See also* Jack Ow, *The Trans-Pacific Partnership's Take on Personal Data* (Dec. 2015), https://www.taylorwessing.com/globaldatahub/article-the-tpp-take-on-personal-data.html.

[127] TPP, *supra* note 3, at art. 14.11.

2. Limits & Potential Risks

Although the TPP has enhanced the harmonization and enforcement of personal data protection rules, it is too early to conclude that it has increased the level of protection of personal data among TPP and non-TPP countries.

First, it seems that the provisions in relation to the privacy of citizens of TPP members are too weak and some key terms remain not clearly defined.[128] For example, Article 14.8.2 explicitly requires that when developing a "legal framework" the framework must include provisions protecting "the personal information of the users of electronic commerce," and provides that each member should "take into account principles and guidelines of relevant international bodies."[129] Here, the issue is that the legal framework presented only applies to "users of electronic commerce," and therefore member states may argue that the framework will not apply to all private sector activities (even if commercial). If so, it will not apply to categories of private sector personal data (such as personal information of employee). The scope of personal data protection requirements is thus, too narrow.[130]

Moreover, the TPP does not mention any specific international instruments that member countries should follow. Neither does it provide a list of principles for members in order to protect personal data nor are any specific enforcement measures mentioned in the TPP. As a consequence, these personal data protection requirements become less enforceable in practice as it is hard for a company or a member to challenge the TPP compliance of other members.

By contrast, as discussed above, the TPP contains detailed provisions to prohibit data export limitations and data localization rules of member states. In comparison with privacy protection provisions, these data export and data localization provisions are definitive and much more like to be enforced.[131] The implications of the data export limitations and data localization provisions for TPP members could mainly benefit cloud-service net exporting countries, particularly the United States by removing those barriers to the data flow through the

---

[128] *See, e.g.*, *id.* at art. 14.8.2 for the meaning of "relevant international bodies."

[129] *Id.*

[130] *See also* Greenleaf, *supra* note 4.

[131] Greenleaf identifies certain exemptions for privacy limitation provisions in the TPP but concludes that they are similarly difficult to enforce. *Id.*

TPP.[132] The provisions would instead, transfer the risks to cloud service net importing countries, such as Australia, Canada, and most of developing country members under the TPP.

The TPP allows U.S. cloud service providers to bypass the TPP members' data localization laws to keep cloud users' personal information on servers in the United States rather than on local servers in other TPP countries, such as in Australia and Canada.[133] This will perhaps deliver an economic advantage to U.S. data storage companies. The ability for US companies to bypass data localization laws may result in both economic and privacy risks for other countries. In particular, this may open the door to further surveillance. As Professor Geist noted, "the combined effect of these U.S. laws is that many users fear that once their information is stored in the U.S., it will be accessible to U.S. authorities without suitable privacy protections or oversight."[134] In fact, even U.S. cloud service providers may share such concerns. In January 2016, Amazon, one of the largest cloud service providers in the world, announced its plans to establish Canadian-based data centers in order to "address mounting fears over the privacy and surveillance implications of information stored in the U.S."[135]

Moreover, the data localization provision (location of computing facilities) could target TPP members' efforts to stop transferring personal data to states with inadequate privacy protections.[136] On October 6, 2015, in *Maximillian Schrems v Data Protection Commissioner* (*Schrems* case), the European Court of Justice issued a landmark ruling that an agreement between the EU and the United States on data sharing, specifically the safe harbor privacy principles[137] is invalid due to

---

[132] U.S. TRADE REP., THE TRANS-PACIFIC PARTNERSHIP: PROMOTING DIGITAL TRADE (FACT SHEET).

[133] Both Australia and Canada has data localization requirement. *See Data Localization Snapshot*, *supra* note 62, at 1.

[134] Geist, *supra* note 65.

[135] Michael Geist, *Thanks to TPP, Canada Could Get Caught in Global Privacy Battle*, THE TYEE (Jan. 19, 2016), http://thetyee.ca/Opinion/2016/01/19/TPP-Global-Privacy-Battle/ (stating this "highlights how businesses and consumers have become increasingly concerned with where their data is transferred and stored.").

[136] Geist, *supra* note 65.

[137] 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 US Department of Commerce, 2000 O.J. (L 215) 7. *See also* Graham Greenleaf, *International Data Privacy Agreements After the GDPR and Schrems*, 139 PRIV. L. & BUS. INT'L REP. 12, 12–15 (2016).

concerns over surveillance activities by United States authorities.[138] The EU court can reach such a decision because it is not a member of the TPP agreement. It is unlikely that a similar decision could be made by any TPP countries due to the effects of the data localization prohibition provisions. Although an increasing number of countries (e.g. EU countries) and businesses (e.g. Amazon) have begun to embrace restrictions on data transfers solely to states with adequate personal data protection, the TPP Agreement could possibly restrict its member states' ability to do the same.[139]

C: IMPLICATION OF DUAL DISPUTE SETTLEMENT MECHANISMS ON CROSS-BORDER DATA PROTECTION

1. Implications to Investors

The TPP provides a greater level of security for investors, but does not render "indirect expropriation of the investment" impossible.[140] The TPP's dual-dispute settlement mechanism would arguably have significant impacts on the investors operating in TPP member states. More specifically, it allows a company in TPP member countries to have more options—such as, have two ways to defend its rights under the TPP: ISDS (Chapter 9) and dispute settlement (Chapter 28).[141] Cross-border personal data protection seems to be the direct focus of the ISDS mechanism as Article 9.6.3 of the TPP explicitly limits the application of ISDS to breach the investment-related provisions under Chapter 9.[142] Regardless, there are still some possibilities for a company to defend its rights under Chapter 14 (in relation to personal data protection) by referring to relevant provisions under Chapter 9 (in relation to the ISDS). For example, as one commentator noted, if a company in one TTP country (e.g. a company in Country A) is not satisfied with the data localization law or policy in another TPP country (Country B), it could claim that Country B has breached the data export limitation or data localization provisions under Chapter 14 of the TPP, and this would

---

[138] Case C-362/14, Schrems v. Data Prot. Comm'r, 2015 O.J. (C 398) 5 (Ir.).
[139] Geist, *supra* note 65.
[140] Greenleaf, *supra* note 4, at 13.
[141] TPP, *supra* note 3.
[142] *Id.*

constitute an "indirect expropriation of the investment" under Chapter 9 Investment, and, therefore, the ISDS regime will apply.[143]

It is also noteworthy that the combined effects of the ISDS and the "most favoured nation (MFN) clause" (i.e. a method of establishing equality of trading opportunity among states by guaranteeing that if one country is given better trade terms by another, then all other states must get the same terms) in the TPP will enable a company from any other TPP countries to make a claim against a TPP member country based on the ISDS provisions in any other trade agreement such a member country has signed, no matter which country (including non-TPP countries) it was signed with.[144] As such, the ISDS possibilities may arguably frighten any TPP member that has laws regarding personal data but a relatively smaller litigation budget than Google or Facebook.[145]

Relating to the implication of disputed settlement mechanism (under Chapter 28), cross-border personal data protection is clearly not the sole focus of the mechanism, and Chapter 28 applies to any breach of TPP provisions.[146] Therefore, any breach of cross-border data transfer provisions under Chapter 14 would arguably be covered by such a mechanism. It is significant that, if a company would like to benefit from this mechanism, it needs to get the support from its government since Chapter 28 only applies to the disputes between member states.

2. Implications to Governments

The potential impacts of dispute settlement systems should not be overstated. Although the TPP contains a dual-dispute settlement mechanism, this does not necessarily mean TPP member countries have to face more disputes in relation to personal data protection. As introduced above, the ISDS mechanism applies exclusively to commitments relating to investment. A breach of any provision, which is not relevant to "investment," will not automatically trigger an ISDS proceeding. In other words, to trigger an ISDS proceeding, the applicant will need to provide sufficient evidence to show the breach of personal data provisions will result in a breach of member's "investment" commitments under Chapter 9.

---

[143] Greenleaf, *supra* note 4, at 13.

[144] Australian Greens Party, *supra* note 118.

[145] *Id.*

[146] TPP, *supra* note 3, at art. 28 (Dispute Settlement).

Although some people are concerned that the ISDS may give foreign investors the right to seek compensation from a TTP member's government, in practice, even if it is an actual breach of the TPP investment obligations, member countries may still be able to avoid ISDS proceedings on various grounds. For example, member governments may justify their data localization policy or law with "legitimate public policy reasons," such as privacy protection, national security, and anti-terrorism.[147] Therefore, so long as a TTP member's government can provide evidence that it acts in good faith, for legitimate public policy reasons, and follows a proper process and national treatment principle, the risk of an ISDS case being taken is very low.[148]

Furthermore, based on a study conducted by the New Zealand government, over the past three decades, New Zealand has had ISDS provisions in international agreements with different countries, including the *NZ-China Free Trade Agreement (2008)*, but no case has ever been taken against it.[149] In Australia, based on the data provided by the Australian government, Australia has signed 28 trade agreements with an ISDS provision, but there has been just one ISDS challenge brought against Australia.[150] Tobacco company, Philip Morris, used an ISDS provision in a Hong Kong-Australia Investment Agreement (1993)[151] to sue the Australian government because of the Australian Tobacco Plain Packaging Act 201. On May 17, 2016 the arbitration tribunal published the decision; the tribunal concluded the arbitration in Australia's favor, and found that Philip Morris Asia's claim was an abuse of process (abuse of rights).[152] This was the first and only ISDS dispute brought against Australia over the past three decades, and Australia won.

Moreover, in a recent study conducted by the Canadian Center for Policy Alternatives in 2015, researchers found that 77 investor-state claims were filed through the NAFTA ISDS system over the past two

---

[147] NEW ZEALAND GOV'T, TPP: IN BRIEF, FACT SHEET (N.Z.) 6 (OCT. 2015), https://www.beehive.govt.nz/sites/all/files/TPP-Q&A-Oct-2015.pdf.

[148] *Id.*

[149] *Id.*

[150] *Investor-State Dispute Settlement*, AUSTL. GOV'T DEP'T OF FOREIGN AFF. & TRADE, http://dfat.gov.au/trade/topics/pages/isds.aspx (last visited Nov. 13, 2016).

[151] Agreement Between the Government of Hong Kong and the Government of Australia for the Promotion and Protection of Investments, Austl.-H.K., Sept. 15, 1993, 1748 U.N.T.S. 385.

[152] *Tobacco Plain Packaging—Investor-State Arbitration*, AUSTL. GOV'T ATT'Y-GEN.'S DEP'T, https://www.ag.gov.au/tobaccoplainpackaging (last visited Nov. 13, 2016).

decades.[153] Canada has been the target of 35 investor-state claims, significantly more than either Mexico (22 claims) or the U.S. (20 claims). Among 35 cases, so far, only three cases have been decided against Canada.[154]As such, the risk for potential ISDS disputes should not be overstated.

D. LIMITED IMPACTS & EXEMPTIONS: LIMITED BY THE NUMBER OF MEMBER COUNTRIES & INTERNET USERS

In terms of cross border data transfer, the influence of the TPP (including both positive and negative impacts) should not be overstated. The TPP has not resolved existing legal challenges relating to cross-border data protection (discussed in Section II), nor has it created any extra challenges which may substantially change the current landscape of personal data protection laws worldwide. In addition, neither the positive impacts of detailed privacy protection provisions nor the negative impacts of the data localization prohibition provisions on offshore personal data protection should be overstated. The impacts of these provisions have been significantly limited by the member coverage of the TPP Agreement. These provisions only apply to twelve TPP member states.[155]

Although these twelve states represent about fourty percent of the world GDP, there is no evidence that shows they also represent a high percentage of world data flow, which is highly relevant to the enforcement of the laws in relation to cross-border data protection.[156] By contrast, based on the data provided by the *Internet Live Stats* on May 8, 2016, the top ten countries on the list of "number of Internet users" are: China, India, United States, Brazil, Japan, Russian, Nigeria, Germany, United Kingdom, and Mexico.[157] Only three of them are TPP member states.[158]

---

[153] SCOTT SINCLAIR, CANADIAN CENTRE FOR POLICY ALTERNATIVES, NAFTA CHAPTER 11 INVESTOR-STATE DISPUTES 29–30 (Jan. 1, 2015), https://www.policyalternatives.ca/sites/default/files/uploads/publications/National%20Office/2015/01/NAFTA_Chapter11_Investor_State_Disputes_2015.pdf.

[154] *Id.* at 29.

[155] TPP, *supra* note 3.

[156] *Id.*

[157] *Internet Users by Country (2016)*, INTERNET LIVE STATS, http://www.internetlivestats.com/internet-users-by-country/ (last visited May 8, 2016).

[158] NEW ZEALAND GOV'T, *supra* note 147, at 1.

Many major economies (non-TPP states but representing a high percentage of internet users), such as the EU, China, and Russia, have all adopted data localization measures in promoting data control.[159] It does not seem that the TPP can "reverse the trend" of data localization. For personal data protection concerns, either joining or withdrawing from the TPP does not greatly impact the current landscape of privacy protection in the cyberspace, including existing challenges brought by cloud computing technology.

E. SUMMARY AND REMARKS: RATIONALE BEHIND & JOIN OR WITHDRAW

In 2016, Professor Graham provided a fine summary of the potential effects of TPP on the protection of the privacy of citizens:

> TPP seems to be the type of binding international privacy treaty that the USA (in particular) wishes to achieve. For the other states whose personal data will be 'hoovered up', it is more likely to be a Faustian bargain: put at risk the protection of the privacy of your citizens (except at home) in return for the golden chalice of trade liberalisation. If the TPP is defeated in the US Congress, this will be a net gain for privacy protection, whatever one thinks about the other potential economic advantages of the TPP.[160]

As discussed above, the TPP does not have substantive or concrete requirements to protect the privacy of citizens of member states.[161] By contrast, it contains detailed provisions to prohibit data export limitations or data localization rules in member states.[162]

The rationale behind this policy decision can easily be identified. The TPP essentially is a "trade" agreement in nature. Accordingly, its main focus is how to strike a trade-off of the economic interests of member states rather than on the equity and justice issues relating to personal data protection. Although it is the first legally binding agreement that provides detailed provisions relating to privacy and personal data protection, it has been highly influenced by the national economic interests of major members. Therefore, people should not have unrealistic expectations of its impacts on the enhancement and harmonization of personal data protection laws in various countries.

---

[159] Mishra, *supra* note 60, at 139.

[160] Professor Graham Greenleaf, *supra* note 4, at 14–15.

[161] *Id.*

[162] *Id.*

Regarding the question whether a country should join or withdraw from the TPP, as discussed, eventually, it seems that this is mainly an economic and political question rather than a citizen rights and privacy law question. For most countries, it is simply a trade-off of economic interests in different industrial sectors, including a trade-off of personal data protection (open digital market by banning data localization rules) and concessions for other industry sectors from other TPP countries (open agriculture market for example).

Using Intellectual property as an example, most of FTAs contain a special chapter on intellectual property (IP).[163] Like many other FTAs, the IP Chapter of the Australia-US FTA (2005) explicitly requires Australia to extend the term of copyright protection to the author's lifetime plus 70 years (it was 50 years).[164] This requirement is certainly positive for the United States, since the United States is a copyright net exporting country. As a copyright net importing country, however, Australia does not have any strong incentive to extend the copyright term. Nevertheless, in order to obtain concessions in other industry sectors from other TPP members (the agriculture sector, for example) Australia eventually agreed to extend its copyright term for another 20 years. It is same for personal data protection provisions under the TPP. There is no incentive for any cloud service net importing countries to ban data localization rules, but they have to accept these provisions in order to get access to the markets of other cloud service exporting countries. Like IP protection, personal data protection is only one of bargaining tools of TPP and other FTA negotiations.

Additionally, although the TPP was successfully concluded, the text of the TPP is still subject to the process of legal review, translation, and verification within each member state. It is generally accepted this should be accomplished within 2 years. It would be interesting to see whether TPP members will still be incentivized to proceed with the ratification of the TPP, particularly, if the United States eventually decides to withdraw from TPP.

---

[163] YIJUN TIAN, RE-THINKING INTELLECTUAL PROPERTY: THE POLITICAL ECONOMY OF COPYRIGHT PROTECTION IN THE DIGITAL ERA 48–56 (2009).

[164] *See* Australia-U.S. Free Trade Agreement, Austl.-U.S., art. 17.4(4), May 18, 2004, 43 I.L.M. 1248, http://dfat.gov.au/about-us/publications/trade-investment/australia-united-states-free-trade-agreement/Documents/Final_text_ausfta.pdf.

V. FUTURE HARMONIZATION - INSIGHTS FROM TPP

Although the vitality of TPP regime is still unclear, and the personal data protection regime under the TPP is full of problems and remains far from perfect, it does provide some insights for future regulators to harmonize international laws on personal data protection and cross-border data flows.

A. CONTENT

In terms of the content of the TPP, *first*, it provides insight on the necessity of unifying legal terms in relation to personal data protection. As mentioned above, the TPP (Art 14.1) provides clear definitions on some key terms in relation to cross-border data protection, such as "computing facilities," "digital product," "electronic transmission," and "personal information."[165] Different countries have different laws regarding personal data protection. Even within a particular country, regulations or industrial rules issued by different authorities could conflict.[166] Therefore, as a starting point for law harmonization, it is an important for all member states to have consensus on the meanings and coverage of some key legal terms in relation of personal data protection.

Second, through detailed provisions on personal data protection in a legally binding international treaty (as introduced above), the TPP actually sets up minimum standards for member states to safeguard personal information/data and ensure the freedom of cross-border data transfer.[167] This may enhance the personal data protection enforcement among all member states, and provides the legal certainty that businesses require to operate in the TPP market.

B. DISPUTE SETTLEMENT MECHANISM & ENFORCEABILITY

In regards to enforcement, the TPP contains a dual dispute settlement mechanism (under Chapter 9 Investment and Chapter 28

---

[165] TPP, *supra* note 3, at art. 14.1.

[166] For example, the definition of 'personal information' could be different under different law and/or ministerial rules in China. *See also* Graham Greenleaf & George Tian, *China Expands Data Protection Through 2013 Guidelines: A "Third Line" for Personal Information Protection, with a Translation of the Guidelines*, 122 PRIVACY L. & BUS. INT'L REP. 1, 2–6 (2013).

[167] Greenleaf, *supra* note 4, at 14–15.

Dispute Settlement).[168] This provides insight on the effective enforcement of personal data protection laws at the international level. Again, using intellectual property rights (IPRs) as a point of comparison, the history of the international protection of IPRs evidenced the significant impact of dispute settlement systems on effective law enforcement. In the 1990s, the *World Intellectual Property Organization* (WIPO) had an inherent institutional deficiency in enforcing the treaties that it oversaw.[169] The introduction of the *Agreement on Trade Related Aspects of Intellectual Property Rights* (TRIPS Agreement) under the WTO framework significantly enhanced international enforcement.[170] This is mainly because Part V of the TRIPS, outlines mandatory dispute settlement procedures and requires that all disputes arising under the Agreement be "settled by the WTO dispute settlement process."[171]

A similar approach can be applied to the possibility of effective international enforcement of personal data protection laws. Like the enforcement IPRs in the 1990s, the extent of privacy/personal data protection and enforcement now varies widely in different nations.[172] The absence of an effective international enforcement mechanism is possibly one of main reasons. By including detailed personal data protection provisions in the TPP (which contain a dual dispute settlement regime), it seems that the United States is attempting to apply a TRIPS strategy (or an IPR international enforcement strategy) to the international enforcement of privacy laws. This approach certainly lends insights for future international privacy law making.

C. BALANCE OF INTERESTS & FLEXIBILITIES

In terms of the flexibility and balance of interests of various stakeholders, as introduced above, the TPP contains some *useful exemptions* for various industries. It also provides specific exemptions for the implementation of the prohibition provision on data exports limitations,[173] and data localization,[174] in order to minimize any

---

[168] TPP, *supra* note 3, at art. 18 (Intellectual Property).

[169] TIAN, *supra* note 163, at 27.

[170] TRIPS, *supra* note 122, at arts. 63–64.

[171] *See id. See also*, TIAN, *supra* note 163, at 31.

[172] *See generally* GRAHAM GREENLEAF, ASIAN DATA PRIVACY LAWS: TRADE AND HUMAN RIGHTS PERSPECTIVES (2014) (providing many fine examples of the various methods of data protection and enforcement).

[173] TPP, *supra* note 3, at art.14.11.

unnecessary interventions of operations of existing personal data protection laws in member states[175]

Additionally, it seems that the TPP is attempting to adopt a WTO-style "Special and differential treatment provisions" to respond to the interest of developing countries.[176] For example, relating to the application of dispute settlement provisions, Article 14.18 (Dispute Settlement) explicitly states:

> 1. Malaysia shall not be subject to dispute settlement under Chapter 28 (Dispute Settlement) regarding its obligations under Article 14.4 (Non-Discriminatory Treatment of Digital Products) and Article 14.11 (Cross-Border Transfer of Information by Electronic Means) *for a period of two years after the date of entry into force of this Agreement for Malaysia.*
>
> 2. Viet Nam shall not be subject to dispute settlement under Chapter 28 (Dispute Settlement) regarding its obligations under Article 14.4 (Non-Discriminatory Treatment of Digital Products), Article 14.11 (Cross-Border Transfer of Information by Electronic Means) and Article 14.13 (Location of Computing Facilities) for a *period of two years* after the date of entry into force of this Agreement for Viet Nam.[177]

In other words, the extra two-year transitional period has been granted to Malaysia and Viet Nam to comply with their obligations on personal data protection under Chapter 14 of the TPP. These strategies (such as "special and differential treatment" strategies) can also be adopted by future regulators in order to better reflect on the interests of developing members in the process of international privacy law making.

D. LETTER OF UNDERSTANDING & EXTRA GUARANTEE

It is noteworthy that the TPP also contains numerous "associated documents" relating to various TPP issues. For example, on February 4, 2016, the United States and Australia exchanged a letter to establish a mutual understanding of privacy protection issues (as a part of the 'TPP

---

[174] *Id.* at art. 14.13.

[175] *See, e.g.*, *id.* at art. 14.3.3.

[176] *See Special and Differential Treatment Provisions*, WORLD TRADE ORG., https://www.wto.org/english/tratop_e/devel_e/dev_special_differential_provisions_e.htm (last visited May 9, 2016).

[177] TPP, *supra* note 3, at art. 14.18.

text and associated documents').[178] In this letter, the United States confirmed:

> Should the U.S. undertake any relevant additional commitments to those in the TPP Agreement with respect to the treatment of personal information of foreign nationals in another free trade agreement, it shall extend any such commitments to Australia. The U.S. will also endeavor to apply extensions of privacy protections with respect to personal information of foreign nations held by the U.S. Government to Australian citizens and permanent residents. [179]

It seems that, by going beyond the commitment of on personal information protection under the TPP, the United States has committed to provide extra protection for personal information held by the US Government to Australian citizens and permanent residents. So long as the United States agrees to offer any extra protection to personal information to any third countries via FTA (such as with the EU), such a protection will apply to Australia automatically. Moreover, the United States appears to have granted Australia with a unilateral most-favored-nation (MFN) treatment on privacy protection for Australians.

It is clear that Australian diplomats have done a fine job in securing privacy protection while in negotiation with their United States counterparts. Since Australia is the only state that has a letter of understanding in relation to privacy protection with the United States, its commitment only applies to Australia (rather than other TPP member states). In terms of future international law making, if such a provision (understanding) were equally and mutually be applied to all member states, it would significantly improve the level of privacy protection worldwide.

E. SUMMARY

In summary, although the privacy provisions in the TPP seem to mainly reflect the economic interests of the United States (as Greenleaf noted) the drafting and negotiation techniques (that are demonstrated in TPP) as well as the legislative strategies (that are adopted by TPP) could be learned from and adopted by future regulators/negotiators, in order to

---

[178] TPP, *supra* note 3 (see 'associate document' session and 'electronic commerce' subsection).

[179] Letter from Michael B.G. Froman, Ambassador, U.S. Trade Representative, to Andrew Robb, Minister for Trade and Inv., Parliament House, Austl. (Feb. 4, 2016), http://dfat.gov.au/trade/agreements/tpp/official-documents/Documents/australia-united-states-privacy-protection.PDF.

help to make an international privacy protection treaty that strikes a better balance between the interests of all member states.

VI. CONCLUSION

This paper has explored the implication of the Internet, particularly cloud computing technology, on cross-border personal data transfers. It particularly examined three major legal challenges that governments, businesses, and individual consumers have to address in the cloud-computing environment: (1) jurisdiction, (2) privacy and security, and (3) convergence. It further examined the new requirements of the TPP in relation to cross-border data transfer and data localization measures, and its implications for existing and future data protection law making.

This article asserts that although the TPP is the "first" international agreement establishing a link between privacy and trade, its impacts should be not overstated. The TPP has not significantly transformed the landscape of international personal data protection laws, nor has provided a direct solution for existing legal challenges of cross-border data protection. To develop an effective solution, it is important to identify and fully understand all potential challenges of cross-border data protection in the current cloud computing and international trade environment, as well as understand the interactions and overlaps between these challenges. In fact, the improvement of public awareness on all potential legal challenges itself could serve as an indispensable part of resolution.

The observation made by Johnson and Post in 1996 is still relevant and valuable in the current cloud computing and digital convergence context:

> Governments cannot stop electronic communication from coming across their borders, even if they want to do so. Nor can they credibly claim a right to regulate the Net based on supposed local harms caused by activities that originate outside their borders and that travel electronically to many different nations. *One nation's legal institutions should not monopolize rule-making for the entire net*.[180]

Within the current globalization and digital convergence environment, it seems that no country can isolate itself from the legal

---

[180] David R. Johnston and David G. Post, *Law and Borders – The Rise of Law in Cyberspace*, 48 STANFORD L. REV. 1367, 1390 (1996).

challenges of cross-border data protection. It is also clear that no single country can address these challenges independently. Due to the transnational nature of cloud technology and the complexity of cross-border data protection, it is important to adopt a more systemic approach, and make domestic and international approaches work collectively to address all potential challenges. Like many other international treaties, regardless of the limits and the sustainability of the TPP regime, it may still serve as a source of laws and provide some useful insights for international privacy law making in the future.