Dark Clouds

Privacy Law as a Barrier to Trade in Cloud Computing

PAPER 9

Table of Contents

I. A Brief Overview of Cloud Computing 3
A. The Historical Development of Cloud Computing 3
B. Defining Cloud Computing 5
II. Privacy Law as a Barrier to Trade 7
III. Analyzing Privacy Laws Under the GATS 12
A. Is Cloud Computing Covered Under the GATS? 12
B. Do Privacy Laws Violate any GATS Obligations? 15
1. Article XVI – Market Access 16
2. Article XVII – National Treatment 17
3. Article VI – Domestic Regulation 21
C. Are Privacy Laws Covered Under any GATS Exceptions? 23
IV. Ensuring the Free Flow of Data Across Borders Through International Cooperation 26
A. Bilateral Agreements 26
B. Regional Agreements 28
C. Multilateral Agreements 30
V. Conclusion 33

INTRODUCTION

The Internet has become an essential tool in facilitating international trade. In 2013, digitally enabled services accounted for 63% of the total cross-border services trade of the United States, having grown from 51% in 2005.[1] An Internet-based service that is rapidly growing in importance is cloud computing. Cloud providers offer various types of computing solutions over the Internet through enormous data centers and are offering them to an increasing number of businesses, from multinational corporations to small- and medium-sized entities (SMEs). In 2012, the global market for public cloud services was $109 billion and is expected to grow to

[1] JAMES MANYIKA ET AL., GLOBAL FLOWS IN A DIGITAL AGE: HOW TRADE, FINANCE, PEOPLE, AND DATA CONNECT THE WORLD ECONOMY 37 (2014), http://www.mckinsey.com/~/media/McKinsey/dotcom/Insights/Globalization/Global%20flows%20in%20a%20digital%20age/MGI_Global_flows_in_a_digial_age_Full_report.ashx.

$237 billion by 2017.[2] In addition, cross-border exports of public cloud services from the United States in 2010 are estimated to be $1.5 billion.[3] These data make clear that cloud computing is a significant and growing part of international services trade. However, the international trade in cloud computing is under threat because of domestic regulations that prevent the free flow of data across borders. Of particular concern are privacy laws that require personal data to be stored domestically or prevent data from being moved across borders. These barriers directly interfere with the service delivery model of cloud providers and thus undermine the possible economic benefits derived from cloud computing.

The main purpose of this paper is to analyze whether these privacy laws are legitimate domestic regulations or are unnecessary barriers to trade in cloud computing. The paper also discusses the current international initiatives being undertaken to facilitate online services trade. Part I of the paper provides a brief overview of cloud computing. Part II discusses how privacy laws interfere with trade in cloud computing. Part III determines whether privacy laws are an unnecessary barrier to trade by analyzing them under the General Agreement on Trade in Services (GATS).[4] Part IV discusses bilateral, regional and multilateral initiatives that seek to ensure the free flow of data across borders and thus guarantee that trade in cloud computing will not be inhibited. Part V provides some concluding remarks.

---

[2] USITC, RECENT TRENDS IN U.S. SERVICES TRADE: 2014 ANNUAL REPORT 75 (2014), *available at* http://www.usitc.gov/publications/332/pub4463.pdf. Public cloud services are usually offered on a time-share or per-use basis to the general public. In contrast, private cloud providers usually offer private entities access to dedicated servers contained within their data centers.

[3] RENEE BERRY & MATTHEW REISMAN, POLICY CHALLENGES OF CROSS-BORDER CLOUD COMPUTING 9 (2012), http://www.usitc.gov/journals/policy_challenges_of_cross-border_cloud_computing.pdf.

[4] General Agreement on Trade in Services, Apr. 15, 1994, 1869 U.N.T.S. 183, 33 I.L.M. 1167 (1994), *available at* http://www.wto.org/english/docs_e/legal_e/26-gats.pdf.

PAPER 9

I. A BRIEF OVERVIEW OF CLOUD COMPUTING

A. The Historical Development of Cloud Computing

Cloud computing has an uncertain history. It is difficult to pin down a singular moment or thinker that initiated the creation of cloud computing. One of the early thinkers that could be said to have contributed to the conceptualization of cloud computing is Douglas F. Parkhill, a Canadian electrical engineer and technologist.[5] In his 1966 book *The Challenge of the Computer Utility*, Parkhill conceived of the idea of a computer industry that provided computing services to the public in the same manner that a public utility, such as an electricity company, provided services. Similar to Parkhill, pioneering computer scientist John McCarthy conceived of computing as a public utility[6] and also contributed the idea of "time-sharing" computers, which would become an important concept for cloud computing.[7] Lastly, another important early thinker was J.C.R. Licklider, one of the pioneers of the Internet, who conceived of the idea of the "intergalactic computer network" that would allow people to access data and applications from anywhere in the world.[8]

Not only is it difficult to determine who came up with the original idea of cloud computing, but there are also competing claims with respect to who first coined the term "cloud computing".[9] Some suggest it was Ramnath Chellappa, an information systems professor, who first used the term "cloud computing" during a talk in 1997.[10] Another source suggests that the

---

[5] *See* Nicholas Carr, *Cloud computing*, BRITANNICA, http://www.britannica.com/EBchecked/topic/1483678/cloud-computing (last visited May 7, 2015).
[6] *See* Ana Cantu, *The History and Future of Cloud Computing*, FORBES (Dec. 20, 2011), http://www.forbes.com/sites/dell/2011/12/20/the-history-and-future-of-cloud-computing/.
[7] *See* John McCarthy, *Reminiscences on the Theory of Time-Sharing*, http://jmc.stanford.edu/computing-science/timesharing.html (last visited May 7, 2015).
[8] *See* Neha Prakash, *Did You Know Cloud Computing Has Been Around Since the '50s?*, MASHABLE (Oct. 26, 2012), http://mashable.com/2012/10/26/cloud-history/.
[9] The "cloud" in "cloud computing" is a reference to the remote data centers that are accessed over the Internet. *See* Antonio Regalado, *Who Coined 'Cloud Computing'?*, MIT TECH. REV. (Oct. 31, 2011), http://www.technologyreview.com/news/425970/who-coined-cloud-computing/.
[10] *See, e.g.*, Cantu, *supra* note 6.

term was invented by either George Favaloro, a marketing executive who allegedly came up with the term in 1996 while working for Comaq Computer, or by John Sullivan, an entrepreneur who tried to trademark the term in May 1997.[11] Regardless of who coined it, the use of the term to describe the group of online computing services recognized today as cloud computing was only popularized when Google and Amazon began using the term in 2006 to describe their services.

Several significant events gave rise to the proliferation of cloud computing. First, in the 1990s, the costs of producing computers was drastically reduced, allowing people to have computers at work and in their homes, and a sufficient amount of bandwidth was deployed to make the Internet a widely accessible resource. These events created the conditions necessary for cloud computing.[12] Second, as cloud computing became commercially viable, many large technology service providers began offering cloud services in the late 1990s and extending into the 2000s:

- Salesforce entered in 1999 to become the first website to deliver applications and software over the Internet;
- Amazon entered in 2002 with its "Web Services" to offer a system of cloud services that included storage and computation and in 2006 introduced the Elastic Computer Cloud (EC2), which permits companies to rent computers that they can use to run their own applications;
- in 2008, Google and Microsoft entered the cloud computing market with Google Apps and Windows Azure, respectively; and lastly

[11] Regalado, *supra* note 9.
[12] *See* Matt Smith, *The History and Development of Cloud Computing*, AEROFS (June 4, 2014), https://www.aerofs.com/blog/the-history-and-development-of-cloud-computing/.

- Apple entered in 2011 with iCloud, which allows users to sync photos, apps, music and documents across various devices.[13]

One of the major drivers of cloud computing demand and innovation today is the proliferation of smartphones and tablets, which allow users to access all their applications and files from the cloud essentially from any location with a wireless Internet connection.[14]

B. Defining Cloud Computing

The National Institute of Standards and Technology (NIST) provides the most generally accepted definition of cloud computing: "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."[15] This definition indicates the features of cloud computing which distinguish it from other online services (i.e., an "on-demand" service which provides "access to a shared pool of configurable computing resources").

In addition, the NIST expands on its definition of cloud computing by providing a list of five essential characteristics:

- *On-demand self-service*. A consumer can unilaterally provision computing capabilities, such as server time and network storage, as needed automatically without requiring human interaction with each service provider.
- *Broad network access*. Capabilities are available over the network and accessed through standard mechanisms that promote use by heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).
- *Rapid elasticity*. Capabilities can be elastically provisioned and released, in some cases automatically, to scale rapidly outward and inward commensurate with demand. To the

---

[13] *See* Prakash, *supra* note 8.
[14] *See* Glenn Blake, *Smartphones, Tablets Spurring Cloud Innovations*, CLOUDTWEAKS (Feb. 26, 2014), http://cloudtweaks.com/2014/02/smartphones-tablets-spurring-cloud-innovations/.
[15] PETER MELL & TIMOTHY GRANCE, NIST SPECIAL PUBLICATION 800-145, THE NIST DEFINITION OF CLOUD COMPUTING 2 (2011), http://csrc.nist.gov/publications/nistpubs/800-145/SP800-145.pdf.

consumer, the capabilities available for provisioning often appear to be unlimited and can be appropriated in any quantity at any time.

- *Measured service*. Cloud systems automatically control and optimize resource use by leveraging a metering capability at some level of abstraction appropriate to the type of service (e.g., storage, processing, bandwidth, and active user accounts). Resource usage can be monitored, controlled, and reported, providing transparency for both the provider and consumer of the utilized service [footnotes omitted].[16]

These five essential characteristics of cloud computing point to the many economic benefits of using cloud services over traditional software and hardware options, especially for SMEs. First, the fact that cloud services are provided on a metered basis allows businesses to have access to advanced computing services without having to incur up-front costs.[17] The ability to obtain service on a metered basis also allows businesses to scale-up or -down as their needs require. This ability to scale-up or -down removes the costs that would be imposed if a business was required to have excess capacity on hand to meet peak demand but which sits idle during non-peak periods. Second, cloud providers are able to leverage large scale economies that arise because of the concentration of equipment, power and management into one central location.[18] Third, cloud computing allows for greater choice for consumers because they have the option of accessing their applications and documents through a plethora of devices, including smartphones and tablets, rather than relying on a single device such as a personal computer.[19] Lastly, depending on the size of the entity, cloud computing may provide a more secure option for storing data.[20] Cloud providers are better able to detect, predict and remedy data security issues because of their ability to attract expertise and leverage scale economies in providing data

---

[16] *Id*.
[17] LEE BADGER ET AL., NIST SPECIAL PUBLICATION 800-146, CLOUD COMPUTING SYNOPSIS AND RECOMMENDATIONS ES-1 (2012), http://csrc.nist.gov/publications/nistpubs/800-146/sp800-146.pdf.
[18] *See* V.V. Arutyunov, *Cloud Computing: Its History of Development, Modern State, and Future Considerations*, 39:2 SCIENTIFIC AND TECHNICAL INFORMATION PROCESSING 173, 175 (2012).
[19] *See* SIIA, GUIDE TO CLOUD COMPUTING FOR POLICYMAKERS 14 (2011), http://www.siia.net/Admin/FileManagement.aspx/LinkClick.aspx?fileticket=PJv7cHdxGTw%3D&portalid=0.
[20] *See id*. at 16.

security. In contrast, an SME would likely find the costs of providing the same level of security offered by a typical cloud provider prohibitively expensive.

The NIST also identifies the three primary service models of cloud providers: Software as a Service (SaaS), Platform as a Service (PaaS) and Infrastructure as a Service (IaaS).[21] The most well-known cloud providers are SaaS providers because they are often public clouds that focus on the general end consumer as their target market. SaaS providers offer software services (e.g., customer relationship management, visual design, word processing, etc.) from the cloud. Notable examples of SaaS products include Salesforce,[22] Google Docs[23] and Dropbox.[24] What distinguishes PaaS providers from SaaS providers is that the former offer an online platform to their customers that they can use to deploy their own applications rather than using those offered by the cloud provider. Examples of PaaS products include Google App Engine[25] and Microsoft Azure.[26] Lastly, IaaS is the most basic cloud computing service model. IaaS providers offer their customers data processing, storage, networks and other fundamental computing resources from the cloud. Amazon EC2 is a notable IaaS product.[27]

II. PRIVACY LAW AS A BARRIER TO TRADE

The two most influential paradigms for privacy law regimes are the United States and the European Union (EU). The United States and EU, however, have fundamentally different approaches to the protection of privacy, both on a theoretical and practical level. On a theoretical level, the EU conceives of privacy as a fundamental human right that protects one's dignity,

[21] Mell, *supra* note 15, at 102.
[22] *See* SALESFORCE, http://www.salesforce.com/ (last visited May 7, 2015).
[23] *See* GOOGLE DOCS, https://docs.google.com/ (last visited May 7, 2015).
[24] *See* DROPBOX, https://www.dropbox.com/ (last visited May 7, 2015).
[25] *See* GOOGLE APP ENGINE, https://cloud.google.com/appengine/docs (last visited May 7, 2015).
[26] *See* MICROSOFT AZURE, http://azure.microsoft.com/en-us/services/websites/ (last visited May 7, 2015).
[27] *See* AMAZON EC2, http://aws.amazon.com/ec2/ (last visited May 7, 2015).

while for the U.S. privacy is an aspect of liberty, particularly liberty from intrusion of the state into one's home.[28] For this reason, the EU places a greater emphasis than the United States with protecting privacy from being infringed by private actors through unauthorized disclosures of information that may embarrass an individual. This fundamental difference explains unique EU privacy rights like the right to be forgotten[29] that is a wholly alien to U.S. privacy law. With respect to the private sector, the United States treats the right to privacy more like an economic right that can be sold or traded like any other property right.[30] The practical consequence of this difference has resulted in the EU taking a broad, cross-sector approach to its privacy legislation,[31] while the United States has only passed sector specific privacy legislation[32] and relies mostly on self-regulation to protect the privacy interests of consumers.[33]

The lack of international consensus on privacy standards has created mistrust among countries that fear putting the protection of their citizens' data in the hands of another country with perceived weaker standards. This mistrust among countries has caused friction in the cross-border flow of data. The inability of data to flow freely across borders has significantly impeded electronic services trade.[34] One of the provisions common in privacy legislation that have been

---

[28] *See* James Q. Whitman, *The Two Western Cultures of Privacy: Dignity Versus Liberty*, 113 YALE L.J. 1151, 1160-64 (2004).

[29] For the leading case on the right to be forgotten, *see* C-131/12, Google Spain SL and Google Inc. v Agencia Española de Protección de Datos (AEPD) and Mario Costeja González, [not yet published], *available at* http://curia.europa.eu/juris/liste.jsf?num=C-131/12.

[30] *See generally* Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393 (1978). *See also* Vernon Valentine Palmer, *Three Milestones in the History of Privacy in the United States*, 26 TUL. EUR. & CIV. L.F. 67, 68 (2011).

[31] The main EU privacy legislation is the European Data Protection Directive, Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the Protection of Individuals with regard to the Processing of Personal Data and on the Free Movement of such Data, 1995 O.J. (L 281) 31.

[32] *See, e.g.*, Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (regulates privacy in the financial sector); Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 (1996) (regulates privacy in the health sector); Children's Online Privacy Protection Act of 1998, 5 U.S.C. §§ 6501–6505 (regulates the online collection of the personal information of children).

[33] *See* Christopher Wolf & Winston Maxwell, *So Close, Yet So Far Apart: The EU and U.S. Visions of a New Privacy Framework*, 26 ANTITRUST 8, 8-10 (2012).

[34] For an attempt at quantifying the economic benefits of removing digital trade barriers, *see* USITC, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 2 100-04 (2014), *available at* http://www.usitc.gov/publications/332/pub4485.pdf.

alleged to impede electronic services trade is the provision requiring the localization of user data or of IT infrastructure such as data centers.[35] For example, privacy laws in two Canadian provinces, British Columbia[36] and Nova Scotia,[37] require public bodies to keep data located within Canada unless one of the few limited exceptions is met. More recently, in July 2014 Russia enacted a law that requires all foreign-owned Internet companies to store the personal data of Russian users within Russia.[38]

Another significant impediment to electronic services trade is privacy legislation that puts restrictions on the transfer of personal data outside a country's borders. A notable example of

---

[35] For an extensive discussion of localization barriers to trade, *see* STEPHEN J. EZELL ET AL., LOCALIZATION BARRIERS TO TRADE: THREAT TO THE GLOBAL INNOVATION ECONOMY (2013), http://www2.itif.org/2013-localization-barriers-to-trade.pdf.

[36] Section 30.1 of the Freedom of Information and Protection of Privacy Act, R.S.B.C. 1996, c. 165, provides:

> A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:
> (a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;
> (b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;
> (c) if it was disclosed under section 33.1 (1) (i.1).

[37] Similar to the British Columbia legislation, s. 5 of the Personal Information International Disclosure Protection Act, S.N.S. 2006, c. 3, provides:

> (1) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless
> (a) where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada;
> (b) where it is stored in or accessed from outside Canada for the purpose of disclosure allowed under this Act; or
> (c) the head of the public body has allowed storage or access outside Canada pursuant to subsection (2).
> (2) The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.
> (3) Where the head of a public body makes a decision pursuant to subsection (2) in any year allowing storage or access outside Canada, the head shall, within ninety days after the end of that year, report to the Minister all such decisions made during that year, together with the reasons therefor.
> (4) In providing storage, access or disclosure of personal information outside Canada, a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body. 2006, c. 3, s. 5.

[38] *See* Paul Sonne & Olga Razumovskaya, *Russia Steps Up New Law to Control Foreign Internet Companies*, WALL ST. J., Sept. 24, 2014, http://online.wsj.com/articles/russia-steps-up-new-law-to-control-foreign-internet-companies-1411574920.

this type of privacy legislation is the EU's Data Protection Directive, which was enacted in 1995. The Directive prohibits the transfer of data to countries that do not provide adequate data protection.[39] The European Commission certifies countries that it determines has adequate protection.[40] Alternatively, businesses can transfer EU data to third countries if they incorporate certain standard clauses into their contracts.[41] Since the United States has not been certified as having adequate data protection, a unique regime was developed in 1998 to cover transfers of EU data to the United States. Under the U.S.-EU Safe Harbor Framework, for U.S. businesses to be able to transfer EU data to the United States they must self-certify that they meet the

[39] Article 25 of the Data Protection Directive provides:

> 1. The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures an adequate level of protection.
> 2. The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.
> 3. The Member States and the Commission shall inform each other of cases where they consider that a third country does not ensure an adequate level of protection within the meaning of paragraph 2.
> 4. Where the Commission finds, under the procedure provided for in Article 31 (2), that a third country does not ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.
> 5. At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 4.
> 6. The Commission may find, in accordance with the procedure referred to in Article 31 (2), that a third country ensures an adequate level of protection within the meaning of paragraph 2 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 5, for the protection of the private lives and basic freedoms and rights of individuals.
> Member States shall take the measures necessary to comply with the Commission's decision.

[40] Andorra, Argentina, Australia, Canada, Guernsey, Israel, Jersey, New Zealand, Switzerland, the Faroe Islands, the Isle of Man and Uruguay have been certified by the EU as having adequate data protection. *See* COMMISSION DECISIONS ON THE ADEQUACY OF THE PROTECTION OF PERSONAL DATA IN THIRD COUNTRIES, http://ec.europa.eu/justice/data-protection/document/international-transfers/adequacy/index_en.htm (last visited May 7, 2015).

[41] *See* Commission Decision 2001/497/EC of 15 June 2001 on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries under Directive 95/46/EC, 1995 O.J. (L 281) 31; Commission Decision 2004/915/EC of 27 December 2004 amending Decision 2001/497/EC as regards the Introduction of an Alternative Set of Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, 2004 O.J. (L 385) 74.

requirements of the Framework.[42] The Federal Trade Commission ensures that businesses that have self-certified under the Framework are continually in compliance. Nevertheless, there is evidence that the Framework has not been working effectively for certain online services, particularly cloud computing.[43] Moreover, the United States is the only country that has a special agreement with the EU for the transfer of EU data and many countries have not been certified as having adequate data protection. For these countries, the EU's Data Protection Directive is effectively as trade restrictive as data localization requirements because it prevents businesses from these countries from transferring EU data across borders.

These aspects of privacy laws directly undermine trade in cloud computing. Imposing data localization requirements on cloud providers forces them to fragment their data centers and prevents them from achieving economies of scale.[44] Furthermore, localization requirements prevent cloud providers from locating their data centers in the most cost-effective locations where land, energy and bandwidth are cheapest.[45] Even in situations where countries use privacy laws to merely impose burdens on the transfer of data across borders, this still imposes substantial compliance costs on cloud providers and can undermine the cost-effectiveness of using cloud computing over traditional software and hardware solutions. Furthermore, burdens imposed by privacy laws on the flow of data across borders also prevent cloud providers from

---

[42] *See* WELCOME TO THE U.S.-EU SAFE HARBOR, http://export.gov/safeharbor/eu/eg_main_018365.asp (last visited May 7, 2015). Close to 5,000 organizations have self-certified under the U.S.-EU Safe Harbor Framework. For a list of these organizations, *see* U.S.-EU SAFE HARBOR LIST, https://safeharbor.export.gov/list.aspx (last visited May 7, 2015).

[43] *See* UNITED STATES DEPARTMENT OF COMMERCE, CLARIFICATIONS REGARDING THE U.S.-EU SAFE HARBOR FRAMEWORK AND CLOUD COMPUTING, http://www.export.gov/static/Safe%20Harbor%20and%20Cloud%20Computing%20Clarification_April%2012%202013_Latest_eg_main_060351.pdf. *See also* USITC, DIGITAL TRADE IN THE U.S. AND GLOBAL ECONOMIES, PART 1 5-13-5-14 (2013), *available at* http://www.usitc.gov/publications/332/pub4415.pdf.

[44] *See* EZELL, *supra* note 35, at 38-39.

[45] *See* BERRY, *supra* note 3, at 18.

optimizing global supply chains.[46] For instance, if a cloud provider has a data center in Japan where it stores data and a data center in the United States where it processes the data, barriers to the free flow of data between Japan and the United States would undermine the cloud provider's ability to transfer data between its two data centers and would negatively affect the quality of the service it could provide to its customers.

III. ANALYZING PRIVACY LAWS UNDER THE GATS

A. Is Cloud Computing Covered Under the GATS?

Determining whether a World Trade Organization (WTO) Member has made a commitment to liberalize a service under the GATS is a complex process. Unlike the General Agreement on Tariffs and Trade,[47] certain obligations under the GATS, notably national treatment[48] and market access,[49] are only applicable if a Member has listed a commitment to liberalize a sector, subsector or activity in its schedule of specific commitments.[50] In addition, commitments are made in accordance with four possible modes of supply:

- Cross-border supply — the possibility for non-resident service suppliers to supply services cross-border into the Member's territory (mode 1);
- Consumption abroad — the freedom for the Member's residents to purchase services in the territory of another Member (mode 2);
- Commercial presence — the opportunities for foreign service suppliers to establish, operate or expand a commercial presence in the Member's territory, such as a branch, agency, or wholly-owned subsidiary (mode 3);
- Presence of natural persons — the possibilities offered for the entry and temporary stay in the Member's territory of foreign individuals in order to supply a service (mode 4).[51]

---

[46] *See* SIIA, *supra* note 19, at 24.
[47] General Agreement on Tariffs and Trade 1994, Apr. 15, 1994, 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994).
[48] *See* GATS, art. XVII.
[49] *See id*., art. XVI.
[50] *See* GUIDE TO READING THE GATS SCHEDULES OF SPECIFIC COMMITMENTS AND THE LIST OF ARTICLE II (MFN) EXEMPTIONS, http://www.wto.org/english/tratop_e/serv_e/guide1_e.htm (last visited May 7, 2015).
[51] *Id*. *See also* GATS, art. 1.

Commitments not to impose any restrictions on a particular mode of supply are listed as "none", while "unbound" is used when a Member wishes to remain free to maintain measures that may conflict with its national treatment or market access obligations. Even if a Member has made a commitment to liberalize a sector, it may still include in its schedule a description of the extent, or conditions under which, it is offering market access or national treatment.

When scheduling commitments, Members are assumed to use either the WTO's W/120 list,[52] the United Nation's Central Product Classification (CPC)[53] or an equally precise classification system unless explicitly stating otherwise.[54] Cloud computing may potentially fall under either "computer and related services" (CPC 84) or "enhanced or value-added telecommunications services" (CPC 7523).[55] Many Members have made commitments under these sector headings.[56] For example, Canada has made full commitments under modes 1 to 3 for both computer and related services and many value-added telecommunications services, including e-mail and online information and data retrieval services.[57]

The Appellate Body has made clear that a service can fall under only one sector or subsector heading. In *US – Gambling*, the Appellate Body held that:

---

[52] *See* World Trade Organization, *Services Sectoral Classification List*, MTN.GNS/W/120 (Jul. 10, 1991), *available at* http://www.wto.org/english/tratop_e/serv_e/mtn_gns_w_120_e.doc.

[53] The version of the CPC in existence at the time the initial GATS commitments were being negotiated was the Provisional Central Product Classification. *See* CPCPROV, http://unstats.un.org/UNSD/cr/registry/regcst.asp?Cl=9&Lg=1 (last visited May 7, 2015).

[54] *See* NELLIE MUNIN, LEGAL GUIDE TO GATS 140 (2010).

[55] *See* BERRY, *supra* note 3, at 21-22.

[56] With respect to computer and related services, 55 Members have made commitments regarding data processing services and 49 have made commitments regarding data base services. In addition, with respect to value-added telecommunications services, 63 Members have made commitments regarding e-mail services and 65 have made commitments regarding online info and data base retrieval services. *See* SACHA WUNSCH-VINCENT, WTO, E-COMMERCE, AND INFORMATION TECHNOLOGIES: FROM THE URUGUAY ROUND THROUGH THE DOHA DEVELOPMENT AGENDA 99, 117 (2005), *available at* http://www.iie.com/publications/papers/wunsch1104.pdf.

[57] CANADA – SCHEDULE OF SPECIFIC COMMITMENTS, https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(@Symbol=%20gats/sc/*)%20and%20((%20@Title=%20canada%20)%20or%20(@CountryConcerned=%20canada))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true# (last visited May 7, 2015).

> [B]ecause a Member's obligations regarding a particular service depend on the specific commitments that it has made with respect to the sector or subsector within which that service falls, a specific service cannot fall within two different sectors or subsectors. In other words, the sectors and subsectors in a Member's Schedule must be mutually exclusive.[58]

Whether a cloud provider's services fall under a specific sector or subsector will be highly contingent on its service model. SaaS providers will most likely fall under computer and related services because their services are similar to software. However, SaaS providers that offer email services, such as Gmail,[59] will more likely fall under value-added telecommunications services. PaaS providers will likely fall under computer and related services, specifically the data processing services (CPC 843) and data base services (CPC 844) subsectors. IaaS providers will likely fall under value-added telecommunications, specifically online and data base retrieval services (CPC 7523).

An issue that may arise when trying to include cloud computing under a Member's schedule of specific commitments is that cloud computing was not yet a commercially viable service at the time of the GATS negotiations. For this reason, some might argue that the negotiators could not have intended to include cloud computing as a commitment. WTO decisions, however, have made it clear that the GATS is technologically neutral with respect to the means of delivery of a service. In *US — Gambling*, the Panel held that the United States' commitment to liberalize the cross-border supply of gambling and betting services included a commitment to liberalize online gambling even though online gambling was not prevalent at the time the GATS was negotiated. The Panel specifically stated that:

> [T]he GATS does not limit the various technologically possible means of delivery under mode 1…[A] market access commitment for mode 1 implies the right for other Members' suppliers to supply a service through all means of delivery,

---

[58] Appellate Body Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶ 180, WT/DS285/AB/R (Apr. 7, 2005).
[59] GMAIL, https://mail.google.com/ (last visited May 7, 2015).

> whether by mail, telephone, Internet etc., unless otherwise specified in a Member's Schedule. We note that this is in line with the principle of "technological neutrality", which seems to be largely shared among WTO Members.[60]

Furthermore, in *China — Audiovisual*, the Appellate Body held that China's commitment to liberalize the "distribution of audiovisual products" included a commitment to liberalize the distribution of these products over the Internet even though at the time of its accession to the WTO Internet distribution of audiovisual products was not a commercially available service.[61] In that case, the Appellate Body explicitly acknowledged that what GATS commitments apply to "may change over time".[62] These WTO decisions provide strong support for the proposition that cloud computing is covered under commitments regarding computer and related services and value-added telecommunications services. Because the commitments are technologically neutral, so long as a service is liberalized, the fact that the service is delivered using cloud technology should not exclude it from protection. Furthermore, since what commitments may be applicable can change over time, the fact that cloud computing was not commercially viable at the time a commitment was made is not a valid ground for excluding it from the commitment.

B. Do Privacy Laws Violate any GATS Obligations?

Assuming that specific commitments have been made, the privacy law provisions described in Part II may potentially violate three GATS obligations: (1) Article XVI – Market Access; (2) Article XVII – National Treatment; and (3) Article VI – Domestic Regulation. Each of these obligations will be addressed in turn.

---

[60] Panel Report, *United States - Measures Affecting the Cross-Border Supply of Gambling and Betting Services*, ¶¶ 6.281, 6.285, WT/DS285/R (Nov. 10, 2004). For an extended discussion of *US — Gambling* and its implications for online services trade, *see* Sacha Wunsch-Vincent, *The Internet, Cross-Border Trade in Services, and the GATS: Lessons from* US—Gambling, 5 WORLD TRADE REV. 319 (2006).

[61] Appellate Body Report, *China - Measures Affecting Trading Rights and Distribution Services for Certain Publications and Audiovisual Entertainment Products*, WT/DS363/AB/R (Dec. 21, 2009).

[62] *Id.* at ¶ 396.

PAPER 9

1. Article XVI – Market Access

The purpose of the market access obligation is to prevent Members from erecting barriers to trade in services through the use of quantitative restrictions. Unlike with goods where tariffs were the primary barrier to trade, in the case of services Members had historically used quota-type restrictions to prevent foreign service suppliers from entering their markets.[63] The Article XVI market access obligation has a two-part structure. First, Article XVI:1 requires that members provide "treatment no less favourable" than that listed in their schedules of specific commitments. This provision thus creates a minimum standard under which Members cannot go under and connects the minimum standard to the commitments listed in a Member's schedule. Second, Article XVI:2 states that where commitments are made Members cannot use certain measures that prevent market access and provides an exhaustive list of such measures.[64]

In *US — Gambling*, the Appellate Body summarized the test for a violation of Article XVI:2 as follows:

> [Article XVI:2 suggests that a complaining Member is] required to make its *prima facie* case by first alleging that the [respondent Member has] undertaken a market access commitment in its GATS Schedule; and, secondly, by identifying, with

[63] WTO — TRADE IN SERVICES 370-71 (Rudiger Wolfrum et al. eds., 2008).

[64] The list of prohibited measures under Article XVI:2 are the following:

> (a) limitations on the number of service suppliers whether in the form of numerical quotas, monopolies, exclusive service suppliers or the requirements of an economic needs test;
> (b) limitations on the total value of service transactions or assets in the form of numerical quotas or the requirement of an economic needs test;
> (c) limitations on the total number of service operations or on the total quantity of service output expressed in terms of designated numerical units in the form of quotas or the requirement of an economic needs test;
> (d) limitations on the total number of natural persons that may be employed in a particular service sector or that a service supplier may employ and who are necessary for, and directly related to, the supply of a specific service in the form of numerical quotas or the requirement of an economic needs test;
> (e) measures which restrict or require specific types of legal entity or joint venture through which a service supplier may supply a service; and
> (f) limitations on the participation of foreign capital in terms of maximum percentage limit on foreign shareholding or the total value of individual or aggregate foreign investment (footnotes omitted).

> supporting evidence, how the challenged laws constitute impermissible "limitations" falling within [Article XVI:2(a)-(f)].[65]

The Appellate Body also elaborated on the meaning of the forbidden measure identified in Article XVI:2(a). Specifically, it had to determine whether a total prohibition on the cross-border supply of online gambling and betting services, which effectively reduced the number of foreign service suppliers to zero, could be considered under Article XVI:2(a) as a limitation "on the number of service suppliers whether in the form of *numerical quotas*, monopolies, exclusive service suppliers or the requirement of an economic needs test [emphasis added]". The Appellate Body held that it could. Among its reasons, the Appellate Body noted that: "[b]ecause zero is quantitative in nature, it can, in our view, be deemed to have the 'characteristics of' a number—that is, to be 'numerical'."[66]

Under this interpretation it is still unclear whether the privacy law provisions identified in Part II would violate Article XVI. Privacy laws do not generally impose quantitative restrictions on service suppliers. Those that place burdens on data being transferred across borders significantly impede cloud providers but they do not prohibit them completely in the same way as the measures scrutinized in *US — Gambling*. A similar argument could be made with regard to privacy laws that require data or servers to be localized. But what if the privacy laws were so onerous that they effectively prohibited all foreign cloud providers from operating in a Member's territory? This situation may come closer to a zero quota but still appears not to be the same as a measure totally prohibiting foreign cloud providers.

2. Article XVII – National Treatment

[65] *US - Gambling*, WT/DS285/AB/R, ¶ 143.
[66] *Id.* ¶ 227.

In contrast to the Article XVI market access obligation, which applies to non-discriminatory measures, the Article XVII national treatment obligation prohibits discriminatory measures. The purpose of national treatment is to ensure that Members do not use measures to discriminate in favor of domestic suppliers over foreign suppliers. Article XVII of the GATS thus plays an analogous role to Article III of the GATT. In fact, the language in Article XVII draws on language used in GATT Article III decisions. For instance, Article XVII:2-3 states:

> 2. A Member may meet the requirement of paragraph 1 by according to services and service suppliers of any other Member, either *formally identical treatment* or formally different treatment to that it accords to its own like services and service suppliers.
>
> 3. Formally identical or formally different treatment shall be considered to be less favourable if it *modifies the conditions of competition* in favour of services or service suppliers of the Member compared to like services or service suppliers of any other Member [emphasis added].

The language in these paragraphs is similar to the language used by the Panel in *U.S. — Section 337 of the Tariff Act of 1930*:

> The words "treatment no less favourable" in [Article III:4] call for *effective equality of opportunities* for imported products in respect of the application of laws, regulations and requirements affecting the internal sale, offering for sale, purchase, transportation, distribution or use of products. This clearly sets a minimum permissible standard as a basis. On the one hand, contracting parties may apply to imported products different formal legal requirements if doing so would accord imported products more favourable treatment. On the other hand, it also has to be recognised that there may be cases where application of *formally identical legal provisions would in practice accord less favourable treatment to imported products* and a contracting party might thus have to apply different legal provisions to imported products to ensure that the treatment accorded them is in fact no less favourable [emphasis added].[67]

Article XVII:2-3 can thus be understood as elaborating on the extent of the "treatment no less favourable" obligation contained in Article XVII:1.

[67] Report of the Panel, *U.S. - Section 337 of the Tariff Act of 1930*, ¶ 5.11, L/6439 (Jan. 16, 1989).

In *EC — Bananas III*, the Panel adopted the following three-part test to determine whether there has been a breach of Article XVII:

> (i) the [responding Member] has undertaken a commitment in a relevant sector and mode of supply; (ii) the [responding Member] has adopted or applied a measure affecting the supply of services in that sector and/or mode of supply; and (iii) the measure accords to service suppliers of any other Member treatment less favourable than that it accords to the [responding Member's] own like service suppliers.[68]

In scrutinizing the privacy law provisions identified in Part II, the main focus will be on whether they accord foreign cloud providers less favorable treatment than domestic cloud providers. The less favorable treatment analysis will depend on several important considerations. First, the fact that a privacy law imposes the same obligations on foreign cloud providers that it imposes on domestic cloud providers is not sufficient to prevent them from breaching Article XVII. Article XVII:2-3 clearly establishes that formally equal treatment between service suppliers may still violate the national treatment obligation if it competitively disadvantages foreign service suppliers. Accordingly, although privacy laws that impose burdens on cross-border flows of data or requirements to localize data or servers provide formally equal treatment, the laws may still violate Article XVII because they are clearly more onerous for foreign cloud providers to comply with than domestic cloud providers.

Second, a Member may try to argue that the less favorable treatment is the result of the inherent competitive disadvantages of foreign cloud providers. Footnote 10 of Article XVII:1 provides that: "Specific commitments assumed under this Article shall not be construed to require any Member to compensate for any inherent competitive disadvantages which result from the foreign character of the relevant services or service suppliers." This qualification of the national treatment obligation ensures that Members are not required to compensate for the fact

[68] Panel Report, *European Communities - Regime for the Importation, Sale and Distribution of Bananas*, ¶ 7.314, WT/DS27/R (May 22, 1997).

that foreign service suppliers may have an inherent disadvantage in providing their services in another market. A Member may argue that the fact that a foreign cloud provider has chosen to locate its data centers outside the domestic market is the reason for its competitive disadvantage in relation to domestic cloud providers. However, in *Canada — Autos*, the Panel ruled that Canadian measures imposing requirements on auto manufacturers to consume a certain level of Canadian services, such as hotel and food and beverage services, in order to qualify for duty exemptions was a violation of Article XVII.[69] Canada tried to argue that footnote 10 of Article XVII:1 immunized the measures because the disadvantages to the foreign service suppliers were inherent.[70] The Panel rejected this argument and held that the purpose of the footnote is to remove any positive obligation on Members to compensate foreign service suppliers for their inherent disadvantages and not to immunize measures that modify the competitive conditions between foreign and domestic service suppliers. Consequently, the footnote would not immunize privacy laws since the measures affect the competitive conditions between foreign and domestic cloud providers independently of any inherent competitive disadvantages resulting from the fact that foreign cloud providers locate their data centers in foreign jurisdictions.

In summary, privacy laws likely violate a Member's Article XVII national treatment obligation. Although burdens on the transfer of data across borders and requirements to localize data and servers are applied equally to both foreign and domestic cloud providers, they nevertheless modify the competitive conditions between them to the disadvantage of foreign cloud providers. This disadvantage results in less favorable treatment to foreign cloud providers compared to domestic cloud providers. Furthermore, footnote 10 of Article XVII cannot be used to immunize a Member's privacy law from scrutiny under its national treatment obligation.

[69] Panel Report, *Canada – Certain Measures Affecting the Automotive Industry*, WT/DS139, 142/R (Feb. 11, 2000).
[70] *Id.* ¶¶ 10.298-10.301.

3. Article VI – Domestic Regulation

Article VI plays a complimentary role to the obligations under Articles XVI to XVII. The Article imposes restrictions on burdensome regulations that impede trade but are neither discriminatory nor restrictive of market access.[71] Because the obligation under Article VI relates to the development and application of regulations (i.e., measures of a qualitative nature), its purpose is analogous to that of the Agreement on Technical Barriers to Trade[72] and Agreement on the Application of Sanitary and Phytosanitary Measures.[73] Article VI has two types of obligations: procedural obligations and substantive obligations. Articles VI:1-3 and 6 impose a positive obligation on a Member to enact adequate procedural protections to ensure that regulations are administered in a reasonable, objective and impartial manner.

Article VI:4-5 contains substantive obligations and has a two-part structure. First, Article VI:4 imposes an obligation on Members to develop sector specific disciplines to ensure that "measures relating to qualification requirements and procedures, technical standards and licensing requirements do not constitute unnecessary barriers to trade in services".[74] Furthermore, the Article provides that the disciplines are to ensure that any requirements or standards imposed by Members are, among other things:

> (a) based on objective and transparent criteria, such as competence and the ability to supply the service;
>
> (b) not more burdensome than necessary to ensure the quality of the service;

---

[71] *See* Wolfrum, *supra* note 63, at 167-68.
[72] *See* Agreement on Technical Barriers to Trade, Apr. 15, 1994, 1868 U.N.T.S. 120.
[73] *See* Agreement on the Application of Sanitary and Phytosanitary Measures, Apr. 15, 1994, 1867 U.N.T.S. 493.
[74] An example of a sector specific discipline is the discipline developed for the accountancy sector, which is still under negotiation as part of the Doha Round. *See* World Trade Organization, *Disciplines on Domestic Regulation in the Accountancy Sector*, S/L/64 (Dec. 17, 1998), *available at* https://docs.wto.org/dol2fe/Pages/FE_Search/FE_S_S006.aspx?Query=(%20@Symbol=%20s/l/*%20and%20@Title=%20accountancy%20or%20(decision%20on%20domestic%20regulation))&Language=ENGLISH&Context=FomerScriptedSearch&languageUIChanged=true#.

> (c) in the case of licensing procedures, not in themselves a restriction on the supply of the service.

Second, Article VI:5 provides that in those sectors where disciplines have not yet been developed, Members are not to apply requirements or standards that "nullify and impair" a specific commitment that has been made. The nullification and impairment assessment is made on a consideration of whether the requirement or standard: (1) does not comply with the factors enumerated in Article VI:4(a)-(c); and (2) could not reasonably have been expected by the Member at the time the specific commitments were made.[75] Commentators have equated Article VI:5 with non-violation nullification and impairment in the context of trade in goods under Article XXIII:1(b) of the GATT.[76] Accordingly, Article VI:5 is violated if a Member makes a specific commitment under its schedule but subsequently enacts a regulatory measure that nullifies and impairs the benefits expected under the commitment.

The crucial question in determining whether privacy laws violate Article VI:5 is whether they meet the condition under Article VI:4(b) of being "not more burdensome than necessary" to meet their regulatory objective. This assessment requires the application of a necessity test, which is applied in many other contexts in the various WTO agreements.[77] The case law suggests that two factors must be examined to determine whether a measure satisfies the necessity test: (1) the contribution of the measure to the realization of the ends pursued by it; and (2) the restrictive impact of the measure on international trade.[78] Although the EU's burdens on the cross-border flow of data are fairly restrictive with respect to electronic services trade, they appear to be reasonably necessary to protect its citizens' data. Once data leave a Member's jurisdiction it becomes significantly more difficult to ensure that they are adequately protected. The EU

---

[75] Article VI:5(b) provides that account should also be taken of the Member's application of international standards.
[76] *See*, *e.g.*, Wolfrum, *supra* note 63, at 193-94.
[77] *See generally* MUNIN, *supra* note 54, at 286-89.
[78] *US - Gambling*, WT/DS285/AB/R, ¶ 306.

privacy regime would be particularly difficult to attack since it permits cross-border data flows in situations where countries are certified as having adequate protections for data. It would be much more difficult to argue, however, that localization requirements for data or servers satisfy the necessity test. These requirements are onerous, particularly for cloud providers who often locate their data centers in jurisdictions that are different from the ones they serve. Furthermore, there are possible alternative solutions that could achieve the same level of privacy protection while imposing less of an impediment to trade in cloud computing. A system where a Member promises to provide the level of privacy protection required by another Member for its citizens' data is such an example.

C. Are Privacy Laws Covered Under any GATS Exceptions?

The purpose of the Article XIV general exceptions is to ensure Members have the regulatory freedom to achieve legitimate public policy goals.[79] In order for a measure to be protected under Article XIV, it has to satisfy a two-part test: (1) the measure must be necessary to achieve one of the enumerated objectives under Article XIV(a)-(e); and (2) the measure must not be applied in a way that would constitute a means of arbitrary or unjustified discrimination where like conditions prevail or a disguised restriction on trade in services as required under the *chapeau* of Article XIV.[80]

With respect to the first step, the most obvious enumerated objective that would be applicable to privacy laws is the one contained in Article XIV(c)(ii), which explicitly provides protection for measures that are "*necessary* to secure compliance with laws or regulations…relating to…the *protection of the privacy* of individuals in relation to the processing and dissemination of personal data [emphasis added]". As stated above, two factors need to be

[79] *See* Wolfrum, *supra* note 63, at 290.
[80] *US - Gambling*, WT/DS285/AB/R, ¶ 292.

examined to determine whether a measure satisfies the necessity test: (1) the contribution of the measure to the realization of the ends pursued by it; and (2) the restrictive impact of the measure on international trade.[81] Both restrictions on the transfer of data across borders and data localization requirements contribute to the compliance of privacy law. These measures ensure that data are adequately protected, which becomes more difficult to do if data were freely transferrable to another jurisdiction. Clearly, however, localization requirements are much more trade restrictive than burdens imposed on cross-border data flows. Less trade restrictive measures are available that may be able to achieve the same level of privacy law compliance (e.g., measures restricting the transfer of data to countries that do not adequately protect privacy). For this reason, localization requirements would likely not meet the necessity test.

Another possibility is that privacy law is exempted under Article XIV(a) for the purpose of protecting public morals and public order. In *US — Gambling*, the Panel provided the following definitions for public morals and public order: "'[P]ublic morals' denotes standards of right and wrong conduct maintained by or on behalf of a community or nation…'Public order' refers to the preservation of the fundamental interests of a society, as reflected in public policy and law. These fundamental interests can relate, *inter alia*, to standards of law, security and morality."[82] The societal interests protected by privacy law would likely place it under the public order exception.[83] Public order potentially has a very broad meaning. For this reason, the exception is limited by footnote 5 of Article XIV(a), which provides: "The public order exception may be invoked only where a genuine and sufficiently serious threat is posed to one of the fundamental interests of society." Nevertheless, because of the importance of privacy to

[81] *Id.* ¶ 306.
[82] *US – Gambling*, WT/DS285/R, ¶¶ 6.465, 6.467.
[83] Some countries that have imposed data localization requirements have explicitly asserted the maintenance of public order as a rationale for the requirements. *See, e.g., Vietnam and the Internet: The audacity of repression*, THE ECONOMIST, August 9, 2013, http://www.economist.com/blogs/banyan/2013/08/vietnam-and-internet/.

modern society and the serious consequences of privacy breaches, this limitation would likely not be sufficient to remove privacy laws from the public order exception. With respect to the necessity test, the analysis provided above regarding whether restrictions on cross-border data flows and data localization requirements satisfy the necessity test for Article XIV(c)(ii) would also apply to Article XIV(b).

The second step of the test required under Article XIV is a determination of whether the measure constitutes a means of arbitrary or unjustified discrimination where like conditions prevail or a disguised restriction on trade in services. The part of the *chapeau* that is most applicable to privacy laws is that dealing with arbitrary or unjustified discrimination. In *US — Shrimp*, the Appellate Body provided a three-part test to determine whether a measure constitutes arbitrary or unjustified discrimination: "First, the application of the measure must result in *discrimination*…Second, the discrimination must be *arbitrary or unjustifiable* in character…Third, this discrimination must occur *between countries where the same conditions prevail* [emphasis original]".[84] Because restrictions on the cross-border flow of data and data localization requirements apply equally to both foreign and domestic cloud providers, it is unlikely that they can be considered discriminatory. For such provisions to violate the *chapeau*, there would need to be evidence of discriminatory application of what are otherwise formally neutral measures.

In summary, restrictions on cross-border data flows and data localization requirements could potentially fall under the Article XIV exceptions dealing with privacy law compliance and public order. Furthermore, these privacy law provisions would likely not violate the *chapeau* since they are formally non-discriminatory. However, data localization requirements could

[84] Appellate Body Report, *United States - Import Prohibition of Certain Shrimp and Shrimp Products*, ¶ 150, WT/DS58/AB/R (Oct. 12, 1998).

potentially be challenged as failing the necessity test because of the existence of less trade restrictive alternatives that achieve the same level of privacy protection.

IV. ENSURING THE FREE FLOW OF DATA ACROSS BORDERS THROUGH INTERNATIONAL COOPERATION

A. Bilateral Agreements

The United States has attempted to encourage the free flow of data across borders by negotiating non-binding e-commerce chapters in many of its bilateral trade agreements. The first such agreement was the U.S.-Jordan Free Trade Agreement.[85] The e-commerce chapter in the agreement is, however, quite brief.[86] The Korea-U.S. Free Trade Agreement (KORUS), the most recent bilateral agreement to contain an e-commerce chapter, has a more extensive non-binding e-commerce chapter.[87] With respect to cross-border data flows, Article 15.8 of KORUS provides: "Recognizing the importance of the free flow of information in facilitating trade, and acknowledging the importance of protecting personal information, the Parties shall endeavor to refrain from imposing or maintaining unnecessary barriers to electronic information flows across borders."

---

[85] Agreement Between the United States of America and the Hashemite Kingdom of Jordan on the Establishment of a Free Trade Area, U.S.-Jordan, Oct. 24, 2000, 41 I.L.M. 63 (2002), *available at* http://www.ustr.gov/sites/default/files/Jordan%20FTA.pdf. *See also* Sacha Wunsch-Vincent, *Trade Rules for the Digital Age*, *in* GATS AND THE REGULATION OF INTERNATIONAL TRADE IN SERVICES 497, 507 (Marion Panizzon et al. eds., 2008).

[86] ARTICLE 7: ELECTRONIC COMMERCE

> 1. Recognizing the economic growth and opportunity provided by electronic commerce and the importance of avoiding barriers to its use and development, each Party shall seek to refrain from:
> (a) deviating from its existing practice of not imposing customs duties on electronic transmissions;
> (b) imposing unnecessary barriers on electronic transmissions, including digitized products; and
> (c) impeding the supply through electronic means of services subject to a commitment under Article 3 of this Agreement, except as otherwise set forth in the Party's Services Schedule in Annex 3.1.
> 2. The Parties shall also make publicly available all relevant laws, regulations, and requirements affecting electronic commerce.
> 3. The Parties reaffirm the principles announced in the U.S.-Jordan Joint Statement on Electronic Commerce.

[87] Free Trade Agreement Between the United States of America and the Republic of Korea, U.S.-S. Kor., Jun. 30, 2007, *available at* http://www.ustr.gov/trade-agreements/free-trade-agreements/jordan-fta/final-text.

Another bilateral trade agreement that may affect trade in cloud computing is the Transatlantic Trade and Investment Partnership (TTIP) agreement currently being negotiated between the United States and the EU.[88] There are some indications that the TTIP will have a significant impact on privacy laws through commitments guaranteeing the free flow of data across borders.[89] However, EU officials have been pushing for the trade deal to contain stronger protections for privacy.[90]

The most recent leaked TTIP text, the EU draft proposal on trade in services, investment and e-commerce for the TTIP negotiations, dated July 2, 2013, contains minimal provisions regarding cross-border data flows.[91] With respect to cloud computing, Article 34 and Section V contain explicit disciplines regarding computer services and electronic communications networks and services, respectively. Privacy is partially addressed in various provisions throughout the text. For example, Article 48 (Confidentiality of information) provides that: "Each Party shall ensure the confidentiality of electronic communications and related traffic data by means of a public electronic communication network and publicly available electronic communications services without restricting trade in services." Furthermore, Article 64(1)(e)(ii) incorporates

---

[88] *See generally* IN FOCUS: TRANSATLANTIC TRADE AND INVESTMENT PARTNERSHIP (TTIP), http://ec.europa.eu/trade/policy/in-focus/ttip/ (last visited May 7, 2015).

[89] *See, e.g.*, Marlon Graff, *ACTA Revisited? TTIP and Data Privacy*, ATLANTIC-COMMUNITY.ORG (Nov. 25, 2014), http://www.atlantic-community.org/-/acta-revisited-ttip-and-data-privacy?redirect=http%3A%2F%2Fwww.atlantic-community.org%2Fyour-opinion%3Fp_p_id%3D101_INSTANCE_GES8xNFE98EL%26p_p_lifecycle%3D0%26p_p_state%3Dnormal%26p_p_mode%3Dview%26p_p_col_id%3Daf-column-1-3%26p_p_col_pos%3D3%26p_p_col_count%3D8; Glyn Moody, *European Parliament Committee Says No To TAFTA/TTIP Deal Without Respect For Data Privacy, But Fails To Offer Snowden Asylum*, TECHDIRT (Feb. 14, 2014), https://www.techdirt.com/articles/20140213/08253226211/european-parliament-committee-says-no-to-taftattip-deal-without-respect-data-privacy-fails-to-offer-snowden-asylum.shtml.

[90] *See EPP Chief Touts Support For TTIP In Parliament; Reding Says Data Deals Key*, INSIDE U.S. TRADE, Mar. 5, 2015.

[91] Petra Pinzler, *EU will laut Geheimdokument Sonderrechte für Konzerne*, ZEIT ONLINE, Feb. 27, 2014, http://www.zeit.de/wirtschaft/2014-02/freihandelsabkommen-eu-sonderrechte-konzerne. However, it is clear from the United States' position in other trade negotiations that it has taken a strong stance on the liberalization of cross-border data flows. As a result, it is unlikely that the United States would accept the limited commitments in the EU proposal.

GATS Article XIV(c)(ii) text permitting measures that secure compliance with privacy laws under the general exceptions. Interestingly, Article 56(1) provides for a seemingly broad commitment regarding the cross-border transfer of data by financial service providers: "Each Party shall permit a financial service supplier of the other Party to transfer information in electronic or other form, into and out of its territory, for data processing where such processing is required in the ordinary course of business of such financial service supplier." However, Article 56(2) limits this commitment by providing that: "Each Party shall adopt appropriate safeguards for the protection of privacy and fundamental rights, and freedom of individuals, in particular with regard to the transfer of personal data." It is unclear how these two seemingly conflicting provisions will interact with each other.

Although the bilateral initiatives are a step forward, they provide only limited benefits to cloud providers. Many situations may arise where a bilateral agreement facilitating cross-border data flows will not benefit a cloud provider. Suppose that the United States and Korea made binding commitments under KORUS to allow unrestricted data flows between the two countries. Many American cloud providers (such as Amazon, which has its data center serving the Asian region in Japan)[92] would not be able to benefit from these commitments because many of their data centers are located in neither Korea nor the United States.

B. Regional Agreements

A notable regional initiative that has attempted to address cross-border flows of data is the APEC Privacy Framework.[93] The Framework is non-binding and principally directed at businesses to

[92] GLOBAL INFRASTRUCTURE, http://aws.amazon.com/about-aws/global-infrastructure/ (last visited May 7, 2015).
[93] Asia-Pacific Economic Cooperation, *APEC Privacy Framework*, APEC#205-SO-01.2 (2005), http://publications.apec.org/publication-detail.php?pub_id=390.

provide guidance for self-regulation.[94] Some issues addressed in the Framework include notice requirements, harm prevention and collection limitations. To complement the Framework, APEC established the Cross-Border Privacy Rules (CBPR) system.[95] The CBPR system

> requires participating businesses to develop and implement data privacy policies consistent with the APEC Privacy Framework. These policies and practices must be assessed as compliant with the minimum program requirements of the APEC CBPR system by an Accountability Agent (an independent APEC CBPR system recognised public or private sector entity) and be enforceable by law.[96]

The CBPR system also allows businesses to self-certify compliance with the APEC Framework and establishes interoperability among the countries that recognize the certification.

Another significant regional agreement that is currently under negotiation and that may address the issue of cross-border data flows is the Trans-Pacific Partnership (TTP).[97] Reports suggest that the U.S. e-commerce proposal contains substantial commitments with respect to measures that restrict cross-border data flows or require localization of data or servers and also contains exceptions modeled on the GATS exceptions.[98] Although TTP parties generally show a willingness to accept the U.S. proposal, some are attempting to water down the commitments by requesting a moratorium on dispute settlement under the e-commerce chapter. Nevertheless, if the U.S. proposal gets incorporated into the TTP, this would be a significant benefit for cloud providers.

---

[94] Section 7 states the Framework is "intended to provide clear guidance and direction to businesses in APEC economies on common privacy issues and the impact of privacy issues upon the way legitimate businesses are conducted. It does so by highlighting the reasonable expectations of the modern consumer that businesses will recognize their privacy interests in a way that is consistent with the Principles outlined in this Framework."
[95] CROSS-BORDER PRIVACY RULES SYSTEM, http://www.cbprs.org/ (last visited May 7, 2015).
[96] *Id.*
[97] *See generally* TRANS-PACIFIC PARTNERSHIP, http://www.ustr.gov/tpp (last visited May 7, 2015).
[98] *See Vietnam Seeks Delay On Enforceability Of TPP E-Commerce Commitments*, INSIDE U.S. TRADE, Nov. 6, 2014.

C. Multilateral Agreements

An early and very influential multilateral initiative that dealt with privacy and data flows is the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980 OECD Guidelines).[99] The 1980 OECD Guidelines were non-binding and addressed such issues as data quality, use specification and use limitation. The Guidelines became the basis for most of the national privacy legislation around the world.[100] In 2013, they were updated and addressed new issues such as data breach notification.[101]

Another multilateral initiative is the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108).[102] Although the negotiators and early signatories of Convention 108 are all members of the Council of Europe, thus making it appear like a regional agreement, the Convention is open to countries who are not members of the Council of Europe. In 2013, Uruguay became the first, and so far only, signatory of Convention 108 that is not a member of the Council of Europe.[103] Convention 108 adopts the EU

---

[99] OECD, OECD GUIDELINES ON THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA, *available at* http://www.oecd.org/internet/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm.

[100] *See* FRED H. CATE ET AL., DATA PROTECTION PRINCIPLES FOR THE 21ST CENTURY: REVISING THE 1980 OECD GUIDELINES 5 (2013), http://www.oii.ox.ac.uk/publications/Data_Protection_Principles_for_the_21st_Century.pdf.

[101] OECD, RECOMMENDATION OF THE COUNCIL CONCERNING GUIDELINES GOVERNING THE PROTECTION OF PRIVACY AND TRANSBORDER FLOWS OF PERSONAL DATA (2013), http://www.oecd.org/sti/ieconomy/2013-oecd-privacy-guidelines.pdf. The following provisions in the revised Guidelines address the cross-border flow of data:

> 16. A data controller remains accountable for personal data under its control without regard to the location of the data.
>
> 17. A Member country should refrain from restricting transborder flows of personal data between itself and another country where (a) the other country substantially observes these Guidelines or (b) sufficient safeguards exist, including effective enforcement mechanisms and appropriate measures put in place by the data controller, to ensure a continuing level of protection consistent with these Guidelines.
>
> 18. Any restrictions to transborder flows of personal data should be proportionate to the risks presented, taking into account the sensitivity of the data, and the purpose and context of the processing.

[102] Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data, CETS No.: 108 (Jan. 28, 1981), http://conventions.coe.int/Treaty/en/Treaties/Html/108.htm.

[103] CONVENTION FOR THE PROTECTION OF INDIVIDUALS WITH REGARD TO AUTOMATIC PROCESSING OF PERSONAL DATA CETS NO.: 108,

approach to privacy protection and thus provides for a high level of protection relative to U.S. standards.[104]

Lastly, the plurilateral Trade in Services Agreement (TISA) currently under negotiation will address cross-border data flows.[105] Several websites have leaked portions of the TISA negotiating text. On June 19, 2014, Wikileaks leaked the Annex on Financial Services.[106] The Annex contains similar language regarding cross-border data flows for financial service providers as that found in the TTIP.[107] In addition, on December 17, 2014, the Associated Whistleblowing Press leaked TISA text containing commitments on data flows.[108] For example, the Article X.4 (Movement of Information) provides: "No Party may prevent a service supplier of another Party from transferring, accessing, processing or storing information, including personal information, within or outside the Party's territory, where such activity is carried out in connection with the conduct of the service supplier's business." Furthermore, Article X.2(iii) prohibits data localization measures. Notably, Article X.7 (Exceptions) does not contain an

---

http://conventions.coe.int/Treaty/Commun/ChercheSig.asp?NT=108&CM=&DF=&CL=ENG (last visited May 7, 2015).

[104] With respect to cross-border flows of data, Convention 108 provides:

> Article 12 – Transborder flows of personal data and domestic law
> 1.The following provisions shall apply to the transfer across national borders, by whatever medium, of personal data undergoing automatic processing or collected with a view to their being automatically processed.
> 2. A Party shall not, for the sole purpose of the protection of privacy, prohibit or subject to special authorisation transborder flows of personal data going to the territory of another Party.
> 3. Nevertheless, each Party shall be entitled to derogate from the provisions of paragraph 2:
> a. insofar as its legislation includes specific regulations for certain categories of personal data or of automated personal data files, because of the nature of those data or those files, except where the regulations of the other Party provide an equivalent protection;
> b. when the transfer is made from its territory to the territory of a non-Contracting State through the intermediary of the territory of another Party, in order to avoid such transfers resulting in circumvention of the legislation of the Party referred to at the beginning of this paragraph.

[105] *See generally* TRADE IN SERVICES AGREEMENT, http://ec.europa.eu/trade/policy/in-focus/tisa/ (last visited May 7, 2015).

[106] *Trade in Services Agreement (TISA): Financial Services Annex*, WIKILEAKS (June 19, 2014), https://wikileaks.org/tisa-financial/WikiLeaks-secret-tisa-financial-annex.pdf.

[107] *See id*., art. X.11.

[108] *Proposal of New Provisions Applicable to All Services of the secret TISA negotiations*, ASSOCIATED WHISTLEBLOWING PRESS (Dec. 17, 2014), https://data.awp.is/filtrala/2014/12/17/19.html.

explicit exception for privacy laws as that found in the GATS. TISA's broad commitments and lack of explicit exception for privacy laws have brought the United States in conflict with the EU with respect to the negotiations.[109]

The ideal situation that would best facilitate trade in cloud computing would be a multilateral privacy protection and cross-border data flows agreement that is incorporated into the WTO. Since there are many philosophical differences with regard to how countries approach privacy protection, it is unlikely that convergence in privacy laws is achievable. More realistic would be a trade-related privacy and data protection agreement within the WTO that facilitated the interoperability of privacy laws.[110] Under this approach, the WTO agreement would ensure a minimum level of protection to data that is transferred among Members.[111] In cases where a Member finds a privacy violation of its citizens' data in a jurisdiction of another Member, the Member where the violation occurred would be obligated to enforce the data protection standards under the agreement and to remedy the violation. Members may decide to provide a higher level of protection if they wish but could not require that other Members apply that level of protection to data transferred to another Member.[112] Having such an agreement under the auspices of the WTO would be important for two reasons. First, having the agreement within the WTO would enable the agreement to achieve broad coverage. This would solve the problem

---

[109] *See U.S. Tackles Restraints On Transfers Of Personal Data In TISA Proposal*, INSIDE U.S. TRADE, Dec. 18, 2014; *Reding Says U.S. E-Commerce Proposal In TISA Falls Short On Privacy, Inside U.S. Trade*, INSIDE U.S. TRADE, Mar. 5, 2015.

[110] This approach to facilitating cross-border data flows is supported by the White House. *See* WHITE HOUSE, CONSUMER DATA PRIVACY IN A NETWORKED WORLD: A FRAMEWORK FOR PROTECTING PRIVACY AND PROMOTING INNOVATION IN THE GLOBAL DIGITAL ECONOMY 31-33 (2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

[111] In the same way the Agreement on Trade-Related Aspects of Intellectual Property Rights provides minimum standards regarding intellectual property protection, the WTO privacy agreement would provide minimum standards regarding privacy protection.

[112] It may even be ideal to have a combination of binding and non-binding agreements. The binding agreement would provide a minimum enforceable standard of protection while the non-binding agreement could be used to address new issues as they arise. The non-binding agreement could be used as the foundation for future updates to the binding agreement. This flexibility is important because privacy laws and data flows affect industries that are highly dynamic. *See* BERRY, *supra* note 3, at 23.

under bilateral agreements of a fragmented global cloud computing market. Furthermore, a privacy and data agreement that applied to all WTO Members, and thus facilitated cross-border data flows among all Members, would allow cloud providers to make decisions on where to locate their data centers based on cost rather than based on regulatory requirements. Second, the WTO's dispute settlement body could be used to settle disputes if there is a complaint that a Member is not providing the minimum level of privacy protection required under the agreement or is impermissibly impeding cross-border data flows.

V. CONCLUSION

This paper analyzed the protections available to cloud providers under the GATS. The analysis, in addition to the subsequent discussion on bilateral, regional and multilateral agreements, reveals that current trade agreements are outdated and inadequate to ensure that trade in online services such as cloud computing is not impaired through the enactment of overly burdensome privacy laws. Although privacy protection is an important societal value, there needs to be more collaboration among countries to find a way to protect privacy in a way that does not unduly interfere with trade in online services. The proposal discussed in the previous section for a WTO privacy and data agreement suggests how WTO Members can achieve the balance between privacy and trade. Although the negotiations for such an agreement would be difficult and contentious, they would likely be no more challenging than the negotiations for the Agreement on Trade-Related Aspects of Intellectual Property Rights. The fact that WTO members were able to come to an agreement on a topic as complex as intellectual property standards suggests they have the capacity to conclude a similar agreement on data and privacy. As services trade becomes more and more reliant on the Internet, such an agreement will become imperative.