

Cross-border Trade of Personal Data: Impact of Privacy Laws on the Private Sector and Analysis under GATS Framework

WAKAKO TAKATORI*

Abstract

This article summarizes the history and development of privacy legislations, i.e., how heightened concern and awareness for the need to protect individuals' privacy led to the adoption and implementation of privacy legislations in many countries. It compares different legal privacy frameworks in three (3) continents, i.e., Europe, the United States and Asia Pacific, and the distinctive nature of privacy legislations in each of these regions. Next, it examines the trade restrictive aspects of privacy laws, i.e., the enactment of privacy laws and their extraterritorial jurisdictional reach in the world of Internet and electronic commerce. It further examines how the privacy compliance requirements, which place restrictions on the free flow of personal data across borders, have affected private businesses, especially the multinational corporations with operations around the globe, at both domestic and international levels. Finally, this article considers the feasibility of creating standard privacy rules to meet the emerging need at the multilateral level, i.e., whether privacy issues could be negotiated at the WTO level and, if so, what would be the optimal method for addressing privacy issues within the GATS framework (where all Members undertake commitments to the harmonized disciplines) in order to facilitate the free movement of personal data in international trade.

1. Introduction

The volume of trade in goods and services across borders has grown at a tremendous speed over the past couple of decades, particularly with the assistance of electronic commerce and the development thereof. As the movement of goods and services naturally involves transfer of data associated with business transactions, there has been an increase in the number of incidents involving inappropriate collection and use of personal information¹ and mishandling of collected personal data.

Inevitably, this has led to substantial harm to individuals who have entrusted their personal data to public and private sectors. As a consequence, an efficient flow of personal information across borders has become a major concern for many individuals and businesses². In response to such an alarming increase in the volume of 'negative' incidents, many countries have adopted and executed personal information protection laws³ at the domestic level.

* The views expressed in this article are the author's own.

¹ Throughout this article, "personal information" and/or "personal data," and the term "privacy" will be used interchangeably.

² Throughout this article, the reference will be "businesses," "private sector," "private business(es)," "private entity(ies)" and/or "multinational corporation(s)."

³ Throughout this article, the reference will be "personal information protection law(s)," "privacy law(s)" and/or "privacy legislation(s)."

As a result, cross-border transfer of personal information, which is necessary for daily business operations for many private entities (especially for multinational corporations with affiliates/subsidiaries located internationally), have become a complicated task. Entities in different countries now face many privacy laws which differ considerably in terms of their scope, applicability, level of restrictions imposed and remedial and enforcement measures.

“Market participants cannot make informed decisions about production, marketing, and investment decisions if they do not know how laws and regulations will affect them. A firm cannot plan and organize its activities efficiently if it does not know in advance what rules it will have to follow.”⁴ In order for private businesses to strategize how best to comply with the privacy requirements and incorporate them as part of their corporate management system, there is a strong need for a clearer guidance, e.g., in the form of the establishment of international privacy standards through a series of negotiations at the multilateral level.

2. Development of Personal Data Protection Legislations

2.1. Development in technology and proliferation of electronic commerce

“Technology has fundamentally changed the way that the businesses are handled by society.”⁵ The development in technology and proliferation of electronic commerce has significantly affected the way in which private businesses carry out their operations. For example, electronic transfer of information across borders has allowed private entities to complete a massive number of business transactions with ease and efficiency. Furthermore, with the introduction of web-based communities, such as Facebook and LinkedIn, individuals around the world have easier access to personal profiles of others by the click of a mouse.

“Because electronic data transfers very easily and takes up infinitely less space than paper, information is being stored not in dusty document warehouses but on laptops, cell phones, voicemail servers, personal digital assistants (PDAs), and backup tapes.”⁶ The development in technology and electronic commerce has not only led to an improved efficiency in how electronic data is collected, processed and stored, but also to a growing number of ‘negative’ incidents where collected personal information is misappropriated.

2.2. Easier access to, and misuse of, personal information

As the number of ‘negative’ incidents has risen at a rapid rate, consumers have started to voice their concerns over the personal information they provide to public authorities and private businesses, i.e., the manner in which their personal data is collected, transmitted as electronic data, stored and used. Consumers’ concerns over the safety of their personal information and the violation of their privacy rights are well described in the comment made by the U.S. Public Interest Research Group as follows.

“In our view, the single, overwhelming barrier to rapid growth of e-commerce is a lack of consumer trust that consumer protection and privacy laws will apply in cyberspace. Consumers...worry, deservedly, that supposedly legitimate companies will take

⁴ PIERRE SAUVÉ, et al. eds., GATS 2000: NEW DIRECTIONS IN SERVICES TRADE LIBERALIZATION, Washington D.C., The Brookings Institution (2000), Chapter 9 Regulatory Reform and Trade Liberalization in Services, pp.225-240, at p.229.

⁵ ALI. Z. MAROSSI, *Globalization of Law and Electronic Commerce Towards a Consistent International Regulatory Framework*, ACM INTERNATIONAL CONFERENCE PROCEEDING SERIES (2006), Vol. 156, Proceedings of the 8th international conference on Electronic commerce: The new e-commerce: innovations for conquering current barriers, obstacles and limitations to conducting successful business on the internet, Fredericton, New Brunswick, Canada, Session: E-government, policy and law track, pp.334-342, at p.336.

⁶ *Id.* at p.336 n.14.

advantage of them by invading their privacy to capture information about them for marketing and other secondary purposes without their informed consent.”⁷

In addition, the development in technology and proliferation of electronic commerce has undoubtedly influenced how governments address (and have addressed) consumer protection issues through their national legislations. Naturally, many governments have made the decisions to adopt and implement privacy laws in response to the public’s concerns over, and its mistrust in the system for, the protection of their personal information and privacy.

2.3. *Enactment of personal data protection legislation*

As the concerns for maintaining the safety and security of individuals’ privacy has grown over the past decades, along with the development in technology and proliferation of electronic commerce, there has been an increasing awareness, among many countries for the need to enact privacy legislations at the national level.

“The global network environment challenges the abilities of each individual country or jurisdiction to adequately address issues related to the electronic commerce and the Internet. The *inherently international nature* of the digital networks and computer technologies that comprise the electronic marketplace requires a global approach to consumer protection as part of a transparent and predictable legal and self-regulatory framework for electronic commerce.”⁸

As a result, many governments started to respond to the calls for taking appropriate measures in order to protect individuals’ privacy. The European Parliament was among the first to adopt privacy legislation, with a view to protect one of the fundamental human rights, i.e., the individuals’ privacy associated with their personal information.

3. Comparative Analysis on Legal Frameworks

3.1. *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 (“EU Directive”)*

In Europe, the right to one’s privacy is considered as one of the fundamental human rights to be legally protected. “The right to privacy is specifically mentioned in a number of constitutions (e.g., Germany and Spain) and in the Council of Europe’s ‘Convention for the Protection of Human Rights and Fundamental Freedoms.’”⁹ Further, as described below, the background information to the development of the EU Directive indicates its focus on protecting individuals’ fundamental rights, i.e., the right to privacy.

The proposal made in the “Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security”¹⁰ confirms this point as follows. Under the proposed approach,

⁷ IL-HORN HANN, KAI-LUNG HUI, TOM S. LEE, I. P. L. PNG, *Online Information Privacy: Measuring the Cost-Benefit Trade-Off*, TWENTY-THIRD INTERNATIONAL CONFERENCE ON INFORMATION SYSTEMS (2002), pp.1-10 (citing to the comment submitted by U.S. Public Interest Research Group in response to call by the U.S. Department of Commerce “Public Comment on Barriers to Electronic Commerce” (65 Fed. Reg. 15,898) Apr. 25, 2000).

⁸ MAROSSO, *supra* note 5, at p.337 (emphasis added).

⁹ BARBARA C. GEORGE, PATRICIA LYNCH, SUSAN J. MARSH, *U.S. Multinational Employers: Navigating Through the “Safe Harbor” Principles to Comply with the EU Data Privacy Directive*, AMERICAN BUSINESS LAW JOURNAL (2001), Vol.38, pp.735-783.

¹⁰ *The Commission Communication on the Protection of Individuals in Relation to the Processing of Personal Data in the Community and Information Security*, Commission of the European Communities, Brussels, COM (1990) 314 final (Sept. 13, 1990) [hereinafter *The Commission Communication*].

one of the objectives of adopting the EU Directive was to “protect the fundamental rights of individuals, and in particular the right to privacy.”¹¹ It further stipulated that “the action taken by the Community must not have the effect of reducing the level of protection but, on the contrary, of ensuring a high level of protection throughout the Community.”¹²

In May 2003, the European Commission issued the “First Report on the Implementation of the Data Protection Directive”¹³ (the “First Report”). The purpose of the First Report was to assess the progress of the implementation of the EU Directive by its Member States¹⁴ and examine whether any amendment to the EU Directive was necessary.

The First Report stated that it had succeeded in fulfilling the “*principle objective of removing barriers to the free movement of personal data* between the Member States.”¹⁵ The First Report further stated that “the main difficulty prior to the adoption of the EU Directive arose because, while most Member States had adopted data protection legislation, a small number had not.”¹⁶

In addition, the problem with respect to the free movement of personal data across the EU Member States’ borders derived not only from the lack of privacy laws in certain Member States, but also the lack of harmonization of these laws at the national level. The First Report recognized this problem and stated that “there might for example be cases where an unnecessarily restrictive rule in one Member State limits the internal processing of personal data in that Member State in the first place and, thus the exportation of the same data to other Member States.”¹⁷ Therefore, the EU Directive clearly envisioned “a world of mainframe computers and trans-border data flows”¹⁸ prior to the development of international trade in the world of Internet and electronic commerce.

In terms of achieving a high level of protection over individuals’ personal data, the First Report confirmed that the EU Directive established some of the highest standards in the world of personal data protection and privacy.¹⁹ At the same time, however, “the [EU] Directive provides stronger requirements for business compliance and legal remedies for violations, but it was designed before the Internet boom and may now be overly rigid.”²⁰

Yet, the First Report identified the importance of balancing two different, but not mutually exclusive, aspects of cross-border transfer of personal data between the Member States, i.e., strong enforcement measures yet simplified compliance requirements to facilitate the flow of transactions across borders. As one of the Commission’s initiatives, the First Report proposed to simplify the requirements for international transfers of personal data, i.e., the requirements for exporting personal data outside the EU to third countries. The First Report affirmed that “[t]he Commission itself intends to make more extensive use of its powers under Article 25(6) and 26(4)

¹¹ *Id.*

¹² *Id.*

¹³ See *The Report from the Commission, First Report on the Implementation of the Data Protection Directive (95/46/EC)*, Commission of the European Communities, Brussels, COM (2003) 265 final, (May 15, 2003) [hereinafter *The First Report*].

¹⁴ When the First Report was issued in 2003, the EU Member States consisted of fifteen (15) countries, including Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxemburg, Netherlands, Portugal, Spain, Sweden and the United Kingdom.

¹⁵ *The First Report*, *supra* note 13, at p.10 (emphasis added).

¹⁶ *Id.*

¹⁷ *Id.*

¹⁸ SWIRE & LITAN, NONE OF YOUR BUSINESS: WORLD DATA FLOWS, ELECTRONIC COMMERCE, AND THE EUROPEAN PRIVACY DIRECTIVE, Chapter 8, Policy Recommendations for Privacy Issues (1998), pp.188-189.

¹⁹ See *The First Report*, *supra* note 13, at p.10.

²⁰ SAUVÉ, et al. eds., *supra* note 4, Chapter 14 Global Electronic Commerce and GATS: The Millennium Round and Beyond, pp.399-437, at p.428.

which provide the best means of simplifying the regulatory framework for economic operators, while ensuring adequate protection for data transferred outside the EU.”²¹

Overall, the EU Directive provides for a comprehensive privacy protection framework, which has been implemented at the national level in all of its Member States²², as opposed to the sectoral and self-regulatory approaches in the United States.

3.2. US Privacy Laws

The US perspective on individuals’ privacy significantly differs from that of the European view, which is based on the concept that privacy is one of the fundamental human rights to be *legally* protected. This difference is apparent from the fact that “there is no specific language about privacy in the U.S. Constitution...”²³ In Europe, the idea is promoted of stringent personal data protection law that punishes violators of one’s privacy rights, while in the United States, there are very few federal or state laws that protect personal information from use by private businesses.²⁴

In the area of personal data protection, the United States has taken a sectoral approach and, as a consequence, “the United States lacks a single, overall, omnibus privacy law.”²⁵ Further, “[d]ata privacy in the United States is covered by intricate legal rules at both the state and federal level.”²⁶ For example, separate federal privacy laws protect individuals’ personal information collected in different industrial sectors.²⁷ In addition, due to the lack of a single, comprehensive set of federal privacy legislation, private entities in the United States face a number of requirements under state laws that regulate the collection and use of personal data, such as anti-spam and telemarketing laws.²⁸

Further, “[t]he United States remains strongly committed to a ‘self-regulatory’ approach to Internet privacy that is favored by its well-organized business community but regarded as completely ineffective and unenforceable by almost all independent privacy advocates and consumer groups.”²⁹ Overall, “[t]he development of [privacy]

²¹ *The First Report*, *supra* note 13, at p.24.

Article 25(6) provides for the Commission’s adequacy findings, i.e., the determination as to whether the level of protection afforded by a third country to which personal data is exported.

Article 26(4) provides for the Commission’s findings as to the sufficiency of standard contractual clauses.

With respect to simplification of the requirements for international transfers of personal data, the Commission, in its First Report, states that it “expects to see progress in four areas: a) a more extensive use of findings of *adequate protection* in respect of third countries under Article 25(6), while maintaining of course an even-handed approach *vis-à-vis* third countries *in line with the EU’s WTO obligations*; b) further decisions on the basis of Article 26(4) so that economic operators have a *wider choice of standard contractual clauses*, to the extent possible based on clauses submitted by business representatives, for example those submitted by the International Chamber of Commerce and other business associations; c) *the role of binding (intra) corporate rules* ... in providing adequate safeguards for intra-group transfers of personal data; d) the more uniform interpretation of Article 26(1) of the Directive ... and the national provisions implementing it.” *The First Report*, *supra* note 13, at pp.24-25 (emphasis added).

²² According to the statement made by the Vice President of the European Commission, Franco Frattini, “[i]ndependent data protection authorities now operate across the 27 Member States of the newly enlarged Europe playing an important role in overseeing data protection principles [under the EU Directive and the EU Charter of fundamental rights].” European Union, Press Release, *Statement from Vice-President Frattini, on behalf of the European Commission, on the occasion of Data Protection Day*, IP/07/102, Brussels (Jan. 28, 2007).

²³ GEORGE, LYNCH, MARSNIK, *supra* note 9, at p.741.

²⁴ *See id.*

²⁵ *Information Technology: As Data Privacy Laws Evolve Globally, Many Nations Consider European Model*, BNA’S INTERNATIONAL TRADE REPORTER, ANALYSIS & PERSPECTIVE (May 1, 2003).

²⁶ SWIRE & LITAN, *supra* note 18, at p.170.

²⁷ *See Information Technology*, *supra* note 25.

For example, the privacy of health information is protected by the Health Insurance Portability and Accountability Act of 1996. The personal information collected by financial institutions is covered by the Financial Services Modernization (Gramm-Leach-Bliley) Act of 1999. The personal information of children collected and processed online is protected by the Children’s Online Privacy Protection Act (COPPA) of 1998.

²⁸ *See id.*

²⁹ SAUVÉ, et al. eds., *supra* note 4, Chapter 14 Global Electronic Commerce and GATS: The Millennium Round and Beyond, pp.399-437, at p.428.

protection [in the United States] has been sporadic, inchoate, sectorially specific and reactive.”³⁰

This US approach, i.e., placing emphasis on adopting market-based and self-regulatory measures to protect personal information, is consistent with the general public view and skepticism toward entrusting its government with activities in the market, especially in the rapidly growing technology areas.³¹

In order to reconcile these different approaches to privacy, the U.S. Department of Commerce and the European Commission entered into an agreed framework called Safe Harbor. “In keeping with the American tradition of privacy protection, Safe Harbor was a reactive response to the threat of an interruption of data transfers between the EU and U.S.”³² “The need to ensure the continued free flow of data out of Europe, and recognition of the large scale of trade between the United States and the European Union prompted the adoption of the safe harbour.”³³

The negotiation between the EU and the United States regarding the adoption of Safe Harbor Principles³⁴, therefore, came about as a result of an effort to balance business needs, i.e., to facilitate the free movement of personal data across borders between the EU and the United States, with political needs (in response to the American public’s mistrust in the system) to abstain from enacting a comprehensive federal privacy legislation (that meets the European adequacy standard for privacy protection³⁵).

3.3. *US Safe Harbor in response to the EU Directive*

On July 27, 2000, the European Commission adopted a decision, indicating that the Safe Harbor Principles provide adequate protection for personal data transferred from the European Union to the United States.³⁶ “Under the Safe Harbor principles, U.S. organizations may *voluntarily* adhere to a set of data protection principles recognized by the European Commission as providing adequate protection. These principles meet the requirements of the EU Directive with respect to transfers of data outside the EU.”³⁷

There are seven (7) principles under the Safe Harbor arrangement negotiated between the United States and the European Union. They are: (1) providing notice of the purpose for which the data is collected and used³⁸, (2) providing choice to opt out or opt in³⁹, (3) providing notice and choice prior to onward transfer to third parties⁴⁰, (4) providing access to personal data collected⁴¹, (5) implementing reasonable security measures⁴², (6) maintaining data integrity in terms of its reliability, accuracy,

³⁰ STEPHEN J. KOBRIN, *The Trans-Atlantic Data Privacy Dispute, Territorial Jurisdiction and Global Governance*, The Wharton School, University of Pennsylvania (Nov. 2002), pp.1-35, at p.11.

³¹ See SWIRE & LITAN, *supra* note 18, at p.187.

³² KOBRIN, *supra* note 30, at p.16.

³³ *Information Technology: EU, U.S. Data Protection Officials, Companies Say Safe Harbor Program A Qualified Success*, BNA’s International Trade Reporter, Europe (Jan. 12, 2006).

³⁴ See *infra* p. 6 and note 37.

³⁵ See Paragraph 1 of Article 25, 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 (the “EU Directive”).

One of the EU Directive’s requirements for the exports of personal data outside EU to a third country is for the importing country ensure “an adequate level of protection” over the data exported from the EU.

³⁶ See Issuance of Principles and Transmission to European Commission: Procedures and Start Date for Safe Harbor List, 65 Fed. Reg. 56,534 (2000).

³⁷ KEVIN P. CRONIN AND RONALD N. WEIKERS, *Data Security and Privacy Law: Combating Cyberthreats*, § 11:6. *European Union Data Protection Directive 95/46/EC—Transfer of personal data outside EU—Safe harbor* (2007) (emphasis added).

³⁸ The United States Department of Commerce, Safe Harbor Website, Safe Harbor Overview, available at http://www.export.gov/safeharbor/eg_main_018236.asp (last visited July 6, 2009).

³⁹ *Id.*

⁴⁰ *Id.*

⁴¹ *Id.*

⁴² *Id.*

completeness and up-to-date content and how the data is used for the stated purpose⁴³ and (7) adopting effective enforcement mechanisms⁴⁴.

In order for an US company to join the Safe Harbor program, “[a] company self-certifies by sending a letter signed by a corporate officer on behalf of the business to the Department of Commerce (DOC) stating that it is joining the safe harbor or by registering online at the DOC website.”⁴⁵ Moreover, in order for private entities in the United States to qualify for the Safe Harbor, they must comply with the above seven (7) principles.

One of the benefits for an US company to comply with the Safe Harbor Principles (which could also be the principal reason why it decides to comply) might be that compliance with the requirements under the Safe Harbor Principles would allow the export of personal data from the EU to the company in the United States, with the underlying assumption that the transfer of personal data satisfies the adequacy standard under the EU Directive.⁴⁶ “Compliance with these rules is backed by the law enforcement powers of the Federal Trade Commission or the Department of Transportation (with respect to airlines).”⁴⁷

As to complaints filed by a EU citizen, alleging a violation of the Safe Harbor Principles by the private business(es) in the US, the complaint and resulting dispute would be referred to “an independent dispute resolution mechanism designated by the U.S. organization at the time it joins the Safe Harbor...”⁴⁸ In addition, businesses in the United States that voluntarily adhere to the principles under Safe Harbor are also subject to the annual reaffirmation requirement, the associated administrative cost of which, understandably, has been one of the major concerns for companies’ top management.⁴⁹

There have been discussions about the level of success as a result of the adoption of Safe Harbor Principles.⁵⁰ At the same time, there have been many criticisms about the lack of comprehensive privacy law in the United States. “In light of the increasing use of high-technology and [the adoption of the EU Directive], the United States must also adopt legislation both to protect citizens against direct marketers that exploit their personal information, as well as to permit U.S. direct marketers to continue to effectively compete in Europe.”⁵¹

As of July 4, 2009, over 1,440 organizations in the United States were listed as certified under the Safe Harbor framework, which was developed by the U.S. Department of Commerce to meet the requirements of the EU Directive.⁵²

3.4. APEC Privacy Framework

In November 2005, the Asia-Pacific Economic Cooperation (the “APEC”) Ministers endorsed the APEC Privacy Framework, which “seeks to ensure the rapid cross-border flow of information and data while protecting consumers, businesses and governments

⁴³ *Id.*

⁴⁴ *Id.*

⁴⁵ GEORGE, LYNCH, MARSNIK, *supra* note 9, at p.766.

⁴⁶ See *Information Technology*, *supra* note 33.

⁴⁷ CRONIN & WEIKERS, *supra* note 37.

⁴⁸ *Id.*

⁴⁹ The US companies that voluntarily adhere to the requirements under Safe Harbor Principles must have external annual audit conducted on its privacy management system, i.e., both the system audit and security audit. This annual re-certification requirement has added to the private businesses’ overall cost of privacy compliance (and has been the major cause of headache for many businesses with multinational operations).

⁵⁰ See e.g., *Information Technology*, *supra* note 33.

⁵¹ JENNIFER L. KRAUS, *On the Regulation of Personal Data Flows in Europe and the United States*, 59 COLUM. BUS. L. REV. 71 (1993).

⁵² The United States Department of Commerce, Safe Harbor Website, The Safe Harbor List, available at <http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list> (last visited July 4, 2009). This number indicates companies whose certification statuses are “current,” and the total number of registered companies, irrespective of their certification statuses, is now up to 1,849. When this article was initially written in July 2007, approximately 1,200 organizations in the United States were registered.

from fraud and criminal activity.”⁵³ In comparison with the EU Directive, “[t]he APEC Privacy Framework promotes a *flexible approach* to information privacy protection for APEC Member Economies, while avoiding the creation of unnecessary barriers to information flows.”⁵⁴

It is important to note that the APEC Privacy Framework aims to maintain a balance between protecting individuals’ personal information and minimizing the potential implementation costs and burdens to be borne by private entities. The APEC Privacy Framework provides for a business-oriented approach to maintaining the information flows across borders, while promoting the accountability⁵⁵ of private businesses for the collection, maintenance and use of personal information for their business operations.

This pragmatic approach contrasts with the approach taken under the EU Directive, which focuses more on the manner in which the personal data should be *protected*, i.e., placing strong emphasis on avoiding misappropriation of collected data. In particular, the EU Directive focuses on the adequacy of the legal system in the importing country to which personal data is exported from the EU.

The APEC Privacy Framework focuses on developing an effective tool in protecting the personal information, which is transferred globally.⁵⁶ The development of such an effective system, in turn, will facilitate the growth of electronic commerce and trade in goods and services across borders.⁵⁷ “[W]hile no APEC decision is [legally] binding [upon its member economies], the standards developed at APEC influence world commerce.”⁵⁸

The APEC Privacy Framework is based on nine (9) principles: (1) preventing harm⁵⁹, (2) maintaining integrity of personal information⁶⁰, (3) providing notice to individuals regarding the purpose for which the personal data is to be collected and used⁶¹, (4) maintaining security safeguards⁶², (5) limiting the collection of personal data to the relevant purposes mentioned in the notice⁶³, (6) providing access to personal information collected and the method for correcting the information⁶⁴, (7) using personal information only for the purposes of collection and other relevant purposes⁶⁵, (8) accountability for compliance with privacy measures⁶⁶ and (9) providing choice to individuals⁶⁷.

⁵³ APEC News Releases, *Ministers Approve APEC Privacy Framework to Strengthen E-commerce and the Protection of Personal Information* (Nov. 16, 2005), available at http://www.apec.org/apec/news___media/2005_media_releases/161105_kor_minsapproveapecprivacyframewrk.html (last visited July 6, 2009).

⁵⁴ *Fact Sheet*, APEC Privacy Framework, APEC Electronic Commerce Steering Group, available at http://www.apec.org/apec/news___media/fact_sheets/apec_privacy_framework.html (last visited July 6, 2009) (emphasis added) [hereinafter *Fact Sheet*].

⁵⁵ Accountability is defined as a responsibility assumed by an organization as a whole in protecting personal data. See MIRIAM H. WUGMEISTER, CYNTHIA J. RICH, *Corporate Privacy Rules: Moving Toward a Global Solution*, 7 PRIVACY & INFO. L. REP. 9 (Oct. 2006).

⁵⁶ At the second APEC Data Privacy Seminar, Australia’s Attorney-General, Philip Ruddock stated that “[p]rotecting personal information is a key to *maintaining consumer confidence, consumer trust and ultimately the business bottom-line*... A system that effectively protects personal information during global data transfers will encourage the growth of e-commerce. That growth facilitates trade; particularly online trade in goods and services.” APEC News Releases, *APEC Makes Progress on Cross-Border Privacy Rules* (June 26, 2007), available at http://www.apec.org/apec/news___media/2007_media_releases/260607_aus_crossborderprivacyprogress.html (last visited July 6, 2009) (emphasis added).

⁵⁷ *See id.*

⁵⁸ MARTIN ABRAMS, *The Strategic Front: Why Should We Care About APEC Implementation*, PRIVACY & DATA SECURITY L. J. (May 2007).

⁵⁹ *Fact Sheet*, *supra* note 54. *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.14.

⁶⁰ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.21.

⁶¹ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.15.

⁶² *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.22.

⁶³ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.18.

⁶⁴ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.23.

⁶⁵ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.19.

⁶⁶ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.26.

⁶⁷ *Id.* *See also* APEC Privacy Framework, part iii, APEC information privacy principles, para.20.

“The APEC [Privacy] Framework has two purposes. The first is to give domestic guidance to economies developing privacy governance regimes... The second, and far more important, purpose to American companies today is to give guidance for privacy mechanisms when data moves across borders.”⁶⁸ The APEC Privacy Framework provides a more *flexible approach* to the movement of personal data across borders than the stringent EU Directive, which makes it almost impossible to transfer personal information if no “adequate” level of protection exists in the importing country.

The APEC Privacy Framework and the language of the Framework “create[] the opportunity for cross border data transfers that are based on an *assessment of a company’s ability to safeguard information, rather than the adequacy of legal systems* where data might be transferred. The [] Directive has proved that the latter is almost impossible.”⁶⁹

This flexible approach under the APEC Privacy Framework has been followed by many countries in Asia Pacific region, where the governments have adopted comprehensive privacy legislations embedded with substantive enforcement mechanisms.

3.4.1. Movement within Asia Pacific Regions

The movement towards implementation of privacy laws in the Asia Pacific region has been rather slow, mainly due to other pressing social, political, economic and infrastructural issues that countries must deal with prior to enacting laws that regulate protection of individuals’ privacy. It is important to note, however, that many countries in the Asia Pacific region, including Australia, Hong Kong and Japan, have already adopted national privacy legislations that regulate the manner in which private entities collect, process, maintain security and use individuals’ personal information.

Australia

The Federal Privacy Act of 1988 (the “Act of 1988”) contains eleven (11) Information Privacy Principles (“IPPs”) which apply to governmental agencies.⁷⁰ On December 21, 2001, the private sector amendments to the Act of 1988 became effective.⁷¹ The new provisions in the amendments to the Act of 1988 provides for ten (10) National Privacy Principles (“NPPs”), which apply to organizations (including non-profit organizations) with an annual turnover of more than three (3) million Australian Dollars (AUD). The provisions also apply to all health service providers regardless of turnover and some small businesses with an annual turnover of three (3) million AUD or less.⁷²

The organizations falling into the above category are now subject to the rules and obligations set forth under the NPPs. The NPPs establish principles on how these private entities must collect, use, protect and disclose individuals’ personal information.⁷³ The NPPs provide individuals with a right to inquire into the type of information an entity maintains about them and a right to correct that information in case it is incorrectly stated.

⁶⁸ ABRAMS, *supra* note 58.

⁶⁹ *Id.*

⁷⁰ See Australian Government, The Office of the Privacy Commissioner, Federal Privacy Law Website, available at <http://www.privacy.gov.au/act/index.html> (last visited July 6, 2009).

⁷¹ *See id.*

⁷² See Australian Government, The Office of the Privacy Commissioner, Federal Privacy Law Website, Private Sector – Business, available at <http://www.privacy.gov.au/business/index.html> (last visited July 6, 2009).

⁷³ See Australian Government, The Office of the Privacy Commissioner, Federal Privacy Law Website, National Privacy Principles (Extracted from the Privacy Amendment (Private Sector) Act 2000), available at <http://www.privacy.gov.au/publications/npps01.html> (last visited July 6, 2009). Ten (10) principles under the NPPs are: (1) Collection, (2) Use and disclosure, (3) Data quality, (4) Data security, (5) Openness, (6) Access and correction, (7) Identifiers, (8) Anonymity, (9) Transborder data flows and (10) Sensitive information.

Australia promotes the NPPs taken from the Act of 1988 and has a Federal Privacy Commissioner to promulgate privacy legislations⁷⁴. In addition, many individual Australian states, including New South Wales, Victoria and Queensland, have adopted their own privacy laws.⁷⁵ New Zealand also has a privacy commissioner and comprehensive privacy legislation.⁷⁶

Principle 9 under the NPPs (“NPP 9”) plays an important role in regulating the global operational aspect of private entities with multinational business practices around the world. “NPP 9 outlines the circumstances in which an organization can transfer personal information it holds to other countries.”⁷⁷ The rules under NPP 9 are based on the EU Directive, which places restrictions on transfer of personal data outside of the EU.

NPP 9 prohibits a company, located in Australia, from transferring personal information (collected within Australia) to others located in the importing country, where the recipients of such data are not subject to “a law, binding scheme or contract which effectively upholds principles for fair handling of the information that are *substantially similar to the [NPPs]...*”⁷⁸ There are exceptions to the rules under NPP 9.⁷⁹

Although the principles under the NPPs provide for a comprehensive framework, as in the case of the EU Directive, “[t]he EU has not granted Australia ‘adequacy status’ regarding the EU Directive...”⁸⁰ At the time the Review of the Private Sector Provisions of the Privacy Act 1988 was conducted and the report was issued, the EU has declared only Argentina, Canada, Guernsey, Isle of Man, Switzerland, the US Safe Harbor Principles, and the transfer of Air Passenger Name Record to the US Bureau of Customs and Border Protection as providing ‘adequate’ privacy protection.⁸¹

Hong Kong

In Hong Kong, the security of personal data is governed by the Personal Data (Privacy) Ordinance (the “Ordinance”), which became effective in December 1996. The Ordinance requires the “data users”⁸² to “safeguard the security of personal data, but does not impose any obligations on data users to notify either the Hong Kong Privacy

⁷⁴ See Australian Government, The Office of the Privacy Commissioner, About the Office, available at <http://www.privacy.gov.au/about/index.html> (last visited July 6, 2009). The “privacy legislations” include the following federal laws: Crimes Act 1914, which regulates the handling of information about old minor convictions; Data-matching Program (Assistance and Tax) Act 1990, which regulates the conduct of federal government data-matching programs; National Health Act 1953, which regulates the handling of Medicare claims information; Telecommunications Act 1997, which monitors disclosures of personal information to law enforcement agencies and consulting on privacy codes.

⁷⁵ See Australian Government, The Office of the Privacy Commissioner, State and Territory Privacy Laws, available at http://www.privacy.gov.au/privacy_rights/laws/ (last visited July 6, 2009).

⁷⁶ See The Office of the Privacy Commissioner, New Zealand, available at <http://www.privacy.org.nz/home.php> (last visited July 6, 2009).

⁷⁷ Australian Government, The Office of the Privacy Commissioner, *Getting in on the Act: The Review of the Private Sector Provisions of the Privacy Act 1988* (Mar. 2005), pp.1-345, at p.76.

⁷⁸ Australian Government, *supra* note 73 (emphasis added).

With respect to the requirements under NPP 9 and the meaning of a “substantially similar” law which is a binding scheme and contract, the Privacy Commissioner stated that it would provide further guidance on how to assess substantial similarity of a privacy regime. See Australian Government, *supra* note 77, at p.80.

⁷⁹ *Id.* “An organization in Australia or an external Territory may transfer personal information about an individual to someone (other than the organization or the individual) who is in a foreign country *only if*: (b) the individual *consents* to the transfer; or (c) the transfer is *necessary* for the performance of a contract between the individual and the organization, or for the implementation of pre-contractual measures taken in response to the individual’s request; or (d) the transfer is *necessary* for the conclusion or performance of a contract concluded in the interest of the individual between the organization and a third party; or (e) the transfer is for the benefit of the individual and the organization can show grounds for a belief that if it were practicable to obtain consent the individual would be likely to give it...” (emphasis added).

⁸⁰ Australian Government, *supra* note 77, at p.74.

⁸¹ See Australian Government, *supra* note 77, at pp.74-75.

⁸² The term “data users” would be the equivalent of “data controllers” covered under the EU Directive 95. The “data user” applies to “any person (data user) that controls the collection, holding, processing or use of personal data.” The Office of the Privacy Commissioner for Personal Data, Hong Kong, The Ordinance at a Glance, available at <http://www.pcpd.org.hk/english/ordinance/ordglance.html> (last visited July 6, 2009).

Commissioner or data subjects of any security breaches that occur.”⁸³ The Ordinance provides individuals the rights to, *inter alia*, obtain a copy of their personal information from the data users, who control the collection, maintenance, processing and use of such data, correct their personal data and complain to the Office of Privacy Commissioner for Personal Data (PCPD) about a suspected violation of the obligations under the Ordinance by the data users.⁸⁴

The PCPD is an independent statutory body which is charged with overseeing the administration, supervision and enforcement of the Ordinance.⁸⁵ It is important to note that one of the PCPD’s duties is to “[I]iaise and cooperate with persons performing similar data protection functions in any place outside Hong Kong in respect of matters of mutual interest concerning the privacy of individuals in relation to personal data.”⁸⁶ The notion of *cooperation* and the *effort to collaborate* with the privacy agency(ies) and governmental authority(ies) in other countries are clearly embedded in the organizational function of the PCPD. This cooperation effort among privacy authorities in many jurisdictions is one of the most important (yet most difficult) objectives to be achieved.

The PCPD receives complaints from individuals whose personal data allegedly has been misappropriated. Upon the receipt of such complaints (or on its own initiative), the PCPD investigates “suspected breaches of requirements of the Ordinance.”⁸⁷ With respect to monitoring the cross-border transfer of personal data outside Hong Kong, there has not been, to date, any complaints or cases brought to the PCPD for investigation.⁸⁸

Japan

On April 1, 2005, the Personal Information Protection Act (the “Act of 2005”) became effective. The Act of 2005 was established to ensure that the rights and interests of individuals would not be violated by inappropriate collection and use of personal information. The Act of 2005 sets forth guidelines for private entities to follow in their practice of personal data collection, processing and use.

In accordance with the Act of 2005, each ministry overseeing a specific industrial sector is responsible for overseeing the privacy practice of that particular industry. For example, the Ministry of Economy, Trade and Industry (METI) has established the Guidelines for Personal Information Protection Laws Concerning Fields of Economy and Industry (the “Guidelines”), which summarize the ways in which the Act of 2005 should be applied in the sectors that METI oversees.⁸⁹ The Guidelines use specific examples to explain what businesses should do to collect, maintain, process, implement security measures and use personal information.

In order for the principles underlying the Act of 2005 to be effective, each holder of personal information must *voluntarily* act to secure the information and ensure its proper handling.⁹⁰ The process of ensuring proper handling and maintaining an appropriate security over collected personal data should be constantly monitored, with the support of

⁸³ MARCUS VASS, SARAH FAIRWEATHER, ANJU MALIK, *Security breaches of personal data in Hong Kong*, Bird & Bird, available at http://www.twobirds.com/English/News/Articles/Pages/Security_breaches_personal_data_HK.aspx (last visited July 6, 2009).

⁸⁴ The Office of the Privacy Commissioner for Personal Data, *supra* note 82.

⁸⁵ *See id.*

⁸⁶ The Office of the Privacy Commissioner for Personal Data, Hong Kong, The Role of the PCPD, available at <http://www.pcpd.org.hk/english/about/role.html> (last visited July 6, 2009).

⁸⁷ *Id.*

⁸⁸ *See* The Office of the Privacy Commissioner for Personal Data, Hong Kong, Case Notes: Complaint & Enquiry Cases related to Transfer of data outside Hong Kong, available at http://www.pcpd.org.hk/english/casenotes/case_complaint2.php?id=116&casetype=B&cid=42 (last visited July 6, 2009).

⁸⁹ The METI oversees economic and industrial sectors.

⁹⁰ *See* The METI Website on Personal Information Protection, available at <http://www.meti.go.jp/english/information/data/IT-policy/privacy.htm> (last visited July 6, 2009).

private organizations.⁹¹ These private organizations are called “Authorized Personal Information Organizations”⁹² and the government is responsible for the certification of these entities.⁹³

Since the enactment of the Act of 2005, consumers as well as private businesses in general have reacted, rather negatively and with panic, to the compliance requirements of this new privacy law. The Act of 2005 has certainly helped raise awareness among the public as to the importance of protecting their privacy and the necessity to ‘keep an eye on’ how businesses, as well as the government, collect and process their personal information. Further, the adoption of this privacy law provided private companies with the opportunity to revisit the manner in which they manage collected personal data, which in turn helped them to better strategize how to maximize the benefits of using the information.

However, there continues to be a need for improvement, by amendments to the Act of 2005 or through other means, in terms of setting a clear standard on transfer of personal data outside Japan, in order both to provide sufficient guidance to private entities with business operations abroad and give consumers the sense of security and confidence in the system.

4. Impacts of Privacy Legislations on the Private Sector

4.1. *The effect of globalization and extraterritorial jurisdictional reach of national privacy legislation on multinational corporations*

As the collection, storage of and access to personal data becomes easier along with the development of electronic storage and commerce over the Internet, many private entities have taken the opportunity of using such data to their business advantage, e.g., by personalizing consumer preferences, making the data available among different departments within the same entity and/or saving the detailed employee data for evaluation and assessment. With respect to consumer data, “[p]ersonal information captured and stored in corporate databases is analyzed, manipulated, shared, and enhanced with other data, allowing organizations to develop customer profiles.”⁹⁴

At the same time, however, there has been an increasing awareness about the appropriateness of collection and maintenance of personal information for business use. “Customers benefit when sound practices and safeguards are in place but when consumer personal information is used haphazardly, violations of rights occur.”⁹⁵

When consumer trust is violated by the misuse and mishandling of their personal data, be it through the inappropriate manner of collecting personal data, the loss of collected data, cybersquatting and/or phishing over the Internet, it not only damages the brand image private entities carry with them but also the relationship and trust that have been built between these businesses and their consumers. For example, “[c]ybersquatting is a driver leading to other abuses that further degrade brand value, customer loyalty and revenues.”⁹⁶ Further, “[the phishing email messages] are helping to undermine confidence in e-commerce for corporations and customers alike.”⁹⁷

One of the main objectives of privacy laws is to ensure the appropriate means of

⁹¹ *See id.*

⁹² *Id.*

⁹³ *See id.*

⁹⁴ KATHY STEWART SCHWAIG, GERALD C. KANE, VEDA C. STOREY, *Compliance to the Fair Information Practices: How are the Fortune 500 Handling Online Privacy Disclosures?*, 43 INFO. & MGMT 805-820 (2006), at p.805.

⁹⁵ *Id.*

⁹⁶ *Cyberspace Lawyer, Major Brands Under Attacks Online*, 12 NO. 6 CYBERSPACE L. 9 (July 2007).

⁹⁷ DAVID BATEMAN, *Phishing for Trouble, Virulent spam mutations threaten your company's good name. Here's how to fight back*, CORP. COUNS. (May 2006), at p.75.

collecting and handling personal information. In addition, the EU Directive has a provision that places a restriction on the transfer of personal data across borders in case the third country, to which such personal data is exported, has no “adequate level of protection” as embedded in the EU Directive.

4.1.1. *Compliance requirements*

The EU Directive establishes certain rules pertaining to the export of personal data outside of the EU Member States. Article 25 of the EU Directive 95 stipulates that: “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*,..., the third country in question ensures an adequate level of protection.”⁹⁸ The EU Directive further stipulates that: “Where the Commission finds, ..., 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.”⁹⁹

The EU Directive, however, does not define the term “adequate level of protection.”¹⁰⁰ This means that the Commission (or national authorities) has discretion to determine the question of whether “adequate level of protection” exists in the third country to which personal data is exported. Data processors in a third country, therefore, have no choice but to accept the “adequate level of protection” standard set by the Commission, if it decides to import such data from any of the Member States. As a consequence, the privacy measure taken by the EU, and its extraterritorial effect on international trade of personal information, could adversely affect trade in services where transfer of personal data across borders is involved (therefore, it becomes a barrier to trade in services when businesses supply different types of services across borders).

4.1.2. *Impediments to trade in services*

The fact that private entities are subject to many different privacy legislations, depending on the level of protection and restriction afforded by privacy law in each country with whom they trade, undoubtedly (and even negatively) affects their strategic marketing plans in a specific region. This may potentially lead to a decline in the volume of goods and services in the world market. For example, with respect to compliance with one of the important elements of any privacy legislations, i.e., obtaining appropriate consent from individuals as to the collection and secondary use of their personal information,

“[o]rganizations that want to transfer personal information legally have only two viable options available to them. They may either obtain the (opt in) consent of the individual concerned or establish a contract with the entity that is receiving the data. In certain situations, however, organizations may be unable to rely on the use of consent or contracts to make their international data transfers... In addition, if consent is required and a customer does not consent, then the organization may not be able to provide the services.”¹⁰¹

To multinational corporations, whose intention upon collection of personal information is to share such data internally¹⁰², i.e., with their branches and/or

⁹⁸ Paragraph 1 of Article 25, the EU Directive (emphasis added).

⁹⁹ Paragraph 4 of Article 25, the EU Directive (emphasis added).

¹⁰⁰ Paragraph 2 of Article 25, the EU Directive. It provides for the basis on which the adequacy of the level of protection is to be assessed.

¹⁰¹ WUGMEISTER, & RICH, *Supra* note 55.

¹⁰² For example, multinational corporations with different types of services (e.g., a multinational company with television broadcasting service, movie production service, home video production service, Internet service and/or merchandizing service) would be able to maximize profits by coordinating their effort on promotional activities, which

subsidiaries located outside the country where the data was originally collected, the requirement to segregate personal data, based on the confirmation of obtaining consent, could pose a technical problem. Moreover, the segregation of collected personal information into two categories, depending on the type of consent obtained, i.e., the first category satisfying either explicit or implicit consent requirement and the second falling under 'data collected with no consent' category, becomes more than burdensome for private businesses in terms of associated cost. For example, businesses are required not only to continue to update the status of individuals' consent, but also to maintain the integrity of both categories of data, i.e., if privacy law allows individuals to request businesses to delete their personal information anytime, businesses will be required to update its databases on a constant basis.

Further, the required structural change within the organization, which is necessary to comply with 'consent requirement' under privacy law (and *only* the consent requirement among other numerous requirements!), will undoubtedly affect the organization's entire strategic planning for marketing, sales and distribution. For example, an enterprise may, in an attempt to avoid the restrictive application of the privacy law to which it is subject, decide to engage in considerably fewer promotional activities so as not to collect any consumer information. Consumers, who used to take advantage of these promotional campaigns by submitting their personal information and, in return, received promotional products and/or services, may see it as a negative consequence arising out of implementation and strict application of the privacy law.

The EU Directive's extraterritorial jurisdictional reach over transfer of data across borders raises another issue, i.e., what if an importing country of such personal data does not have (or has not adopted) privacy law that affords "adequate level of protection" within the meaning of Article 25 of the EU Directive? The adoption of stringent privacy legislation, such as the EU Directive, might adversely affect countries where no "adequate" privacy law exists. "The issue could have an impact on developing countries' exports of data- processing services, and it poses a difficult choice for these countries. If they choose not to enact laws that are deemed adequate, they could be shut off from participation in this growing market [i.e., EU]."¹⁰³

In addition, "[t]he effect of extraterritorial application of the [EU] Directive on U.S. multinational employers, and businesses in general, could be catastrophic."¹⁰⁴ For instance, a multinational corporation that operates in Europe routinely collects and processes personal information of its employees as part of its daily business operations. If the main server, containing all of its employee data, is in the United States, the personal data collected and processed in Europe must be transferred across borders in the virtual electronic world. The EU Directive, then, "would have a profound effect on human resources operations in U.S. companies conducting business in the EU by preventing much of the compilation and transfer of personal information that is a frequent occurrence in human resource departments."¹⁰⁵

If a country has not adopted an appropriate (or "adequate") privacy law, and if it is not in line with the existing legal system and infrastructure in that country, it would be more than difficult for private entities in that country to commit their practice in accordance with the required standard established in their trading-partner countries. "If [countries with no existing privacy law] do [decide to] enact stringent laws, then, unless

target on a certain group of consumers. This synergy effect would be possible by making the most efficient use of consumer data collected and stored in the company's database.

¹⁰³ BERNARD HOEKMAN, et al. eds., *DEVELOPMENT, TRADE, AND THE WTO: A HANDBOOK*, Washington D.C., The World Bank (2002), Chapter 29, Domestic Regulations and Liberalization of Trade in Services, at p.292.

¹⁰⁴ GEORGE, LYNCH, MARSNIK, *supra* note 9, at pp.737-738.

¹⁰⁵ *Id.*, at p.738.

the laws can be made specific to trade with particular jurisdictions, the result could be an economy-wide increase in the costs of doing business.”¹⁰⁶

Because the EU Directive makes it a condition upon non-European countries to afford “adequate” level of protection over personal data they import from the EU, “[a]ccess to the enormous EU market will depend on compliance with data protection laws.”¹⁰⁷ The EU Directive, then, may serve as a trade protectionist measure against the flow of personal data across borders and it may be viewed, by many non-EU countries, as creating unnecessary barriers to trade.

4.1.3. *Costs and benefits of compliance*

The compliance effort by private entities involve, among others, taking specific steps to achieve personal information protection goals within the enterprises. “Examples would include policies adopted by senior management, training programs for personnel, and specific security measures adopted with respect to access to personal data.”¹⁰⁸ Therefore, in order for these businesses to strategize their market plans and assess the importance of complying with privacy laws, i.e., not only domestic privacy laws but also privacy laws of foreign countries in which they conduct business operations, the cost and benefit analysis becomes the most important and decisive factor.

Costs

The cost that private entities incur in order to comply with privacy legislation is substantial. They not only must be cautious about full compliance with their domestic privacy law, but also the law of the country from which they import personal data. As a result of the high administrative and regulatory burden to private entities involved in cross-border trade, they may significantly be discouraged to comply with (any) privacy law. Many companies in the United States, for example, that are subject to the annual audit requirement¹⁰⁹ have felt that the cost to conduct such external audit process is too high. “Some [companies may] opt to try and fly under the radar and hope they will not be caught violating data privacy laws. Others [may] fashion a compliance program that is tailored only to comply with the countries in which they operate.”¹¹⁰

The following may help illustrate a complex web of *full* compliance with privacy laws in different jurisdictions. A multinational corporation with branches in fifteen (15) EU Member States, Japan, the United States and Canada wishes to maintain a centralized consumer database to provide the most efficient global customer services; however, this corporation would be required to enter into seventy-nine (79) separate contracts among its affiliates and to have eighteen (18) different privacy notices, in order to fully comply with the privacy requirements in each of these countries.¹¹¹

Furthermore, if an organizational change in any of these branches takes place, new contracts will need to be signed. If this multinational corporation decides to rely on the consent of individuals who provided their personal data to the company, then it must permit these individuals to withdraw their consent at any time and maintain the updated list of their consent preferences. Because the administrative and procedural costs of complying with the requirements under privacy legislations in many different countries

¹⁰⁶ M. AADITYA AND W. SACHA, *Preempting Protectionism in Services: The GATS and Outsourcing* (Jan. 2004), p.11.

¹⁰⁷ SWIRE & LITAN, *supra* note 18, at p.154.

¹⁰⁸ *Id.*, at p.165.

¹⁰⁹ For example, private entities in the United States, which self-certify and commit to the Safe Harbor Principles, must go through an annual external audit process in order to reaffirm their privacy compliance with the Safe Harbor Principles.

¹¹⁰ *Information Technology*, *supra* note 25.

¹¹¹ See WUGMEISTER, & RICH, *Supra* note 55.

could be so expensive and burdensome, it might be easier for the company not to provide the most efficient customer service.¹¹²

“Globalization and international factor mobility has implications for efficient transactions of firms operating in multiple jurisdictions.”¹¹³ The compliance cost to a multinational corporation would certainly have a significant impact on the way in which it conducts business around the world. The high costs associated with full compliance in several jurisdictions, with varying degrees of requirements, may not result in, and may even prevent businesses from, providing goods and services in an efficient (if not the most efficient) manner.

Benefits: improvement in the companies’ privacy management system

The survey conducted on executives in industries handling personal information indicated that, “rather than take a leadership position, [these executives] wanted to adopt privacy policies only when a consensus had developed in their industry or laws had been passed.”¹¹⁴ The multinational companies, which handle processing of personal information, are legally bound to comply not only with the terms and conditions in the contracts but also with the applicable privacy legislations in exporting and importing countries. The jurisdictional reach of a country’s national privacy legislation becomes an important factor for private entities, with operations in multiple jurisdictions, to assess the efficiency of business transactions.

The effective management of personal information, therefore, provides private entities with a chance to revisit their existing corporate policies and make necessary changes to handle such data in the most efficient, secure and profitable manner. If no such corporate policy exists, the businesses can adopt a new set of privacy policies and assess how they can effectively incorporate the privacy compliance requirements into their business practice.

Benefits: improvement in the quality of goods and services

Moreover, “[t]he[] cross-border limitations are affecting both the quality and choice of products and services that can be offered to consumers on a global basis.”¹¹⁵ The private entities that face a number of compliance rules are subject to more rigorous quality inspections and better consumer communications. This, in effect, would lead to the improvement in the quality of customer care provided and/or the quality of goods and services circulated in the global market.

Benefits: improvement in the level of confidence entrusted by consumers

The privacy policy statements by companies (e.g., on their websites) provide consumers with the assurance on how their personal information is collected, maintained, processed and used. In order for these companies, not only to comply with the law, but also to continue to serve their consumers with the trust they place in the way their information is handled, the companies must follow the best practice in accordance with their privacy policy statements.

4.2. Role of contracts

As part of self-regulatory scheme, private entities may choose to incorporate standard terms of reference in their contracts, where particular business transactions involve movement of personal information across borders, in order to subject themselves

¹¹² See WUGMEISTER, & RICH, *Supra* note 55.

¹¹³ MAROSS, *supra* note 5, at p.336.

¹¹⁴ H. JEFF SMITH, *Privacy Policies and Practices: Inside the Organizational Maze*, Communications of the ACM, Vol.36, No.12 (1993).

¹¹⁵ WUGMEISTER, & RICH, *Supra* note 55.

to a set of obligations under a certain privacy regime. Model contracts, for example, “refer to efforts to provide standard terms for transferring data.”¹¹⁶ Companies may elect to incorporate model contracts and the standard contractual clauses thereof word-for-word, or they may incorporate the standard terms into separate contracts with necessary additions or modifications to satisfy the special conditions of parties involved.¹¹⁷

According to the Commission Staff Working Document¹¹⁸ on standard contractual clauses for the transfer of personal data to third countries, the European Commission adopted the “business clauses”¹¹⁹ that have been supported by the representatives of data controllers. “The new set of standard contractual clauses [allow data exporters and data importers to] choose between two different sets for transfers controller-to-controller and one set for controller-to-processor.”¹²⁰ The European Commission expects that, with this new set of standard contractual clauses that fit more to the business operations of private entities, the use of standard contractual clauses will increase in Europe.¹²¹

However, there are practical difficulties in ascertaining the recipients’ non-compliance with the standard contractual terms, especially when a recipient third country has no effective supervising and/or enforcement authority. The lack of an appropriate supervising and/or enforcement body becomes a problem where the only basis individuals have to bring claims for violation of their privacy rights is the standard terms of contract. Therefore, designing the process for resolving disputes between individuals and private companies that have adopted the self-regulatory measure is another issue that must be addressed in the absence of effective supervisory and/or enforcement mechanism.

4.3. *Harmonized privacy standards*

The need to establish harmonized rules with respect to privacy protection at the multilateral level has become one of the major issues to be considered by many privacy professionals. One important aspect in relation to the harmonization of rules at the global level is the coordination efforts to be made among data protection officials. “The meetings of international [privacy] commissioners are especially important because of the increasingly global nature of information flows, especially for electronic commerce, and the consequent large spillover effects of national and EU data protection laws.”¹²²

Establishing the standard disciplines and obligations with respect to cross-border transfer of personal data would certainly benefit the countries involved in the goods/services trade, as well as the important players in the global marketplace, i.e., private businesses and multinational corporations. The following section, therefore, will examine a prospect for addressing privacy issues within the existing rules and obligations under WTO law, namely the GATS.

5. Prospect for Harmonization of Privacy Legislations

5.1. *Possibility of multilateral negotiation within the framework of the GATS – The relationship between WTO and privacy*

¹¹⁶ SWIRE & LITAN, *supra* note 18, at p.157.

¹¹⁷ *See id.*

¹¹⁸ The Commission Staff Working Document on the Implementation of the Commission Decisions on Standard Contractual Clauses for the Transfer of Personal Data to Third Countries, (2001/497/EC and 2002/16/EC), Commission of the European Communities, Brussels, SEC (2006) 95, (Jan. 20, 2006) [hereinafter *Working Document*], at p.7.

¹¹⁹ *Id.*

¹²⁰ *Id.*

¹²¹ *See id.*

¹²² SWIRE & LITAN, *supra* note 18, at p.182.

The advance in Internet technology, and an ever-growing volume of electronic trade that naturally followed this technological development, has led to the proliferation of electronic delivery of services across borders.¹²³ This proliferation of trade via electronic means has shed light on a number of underlying issues regarding the effectiveness and adequacy of existing international trade laws and regulatory mechanisms.¹²⁴ For example, with respect to the WTO Members' willingness to resort to the rules and obligations under the GATS, there has been a continuing reluctance among WTO Members to bring cases under the GATS.¹²⁵ As a result, some of the fundamental concepts of the GATS remain, at its best, obscure.¹²⁶ "This significantly weakens the function of the GATS, which is supposed to provide a framework for the ever-growing cross-border service trade."¹²⁷

The reason for Members' reluctance to bring cases in accordance with the dispute settlement procedures could be that "trade obligations usually are not directly binding in domestic law, and trade agreements leave considerable scope for each country to implement its obligations in the way it sees fit."¹²⁸ "Law has traditionally been the province of the nation state, whose courts and police enforce legal rules. By contrast, international law has been comparatively weak, with little effective enforcement powers."¹²⁹ However, the rapidly growing environment in electronic commerce continues to question each sovereign nation's abilities to address issues, which are associated with electronic transfer of goods and services across borders.

In parallel with the concept of autonomy of sovereign nations to regulate their own laws, there has been a challenge to the effectiveness and sufficiency of existing legal framework in the area of international trade. This is certainly the case in the world of electronic commerce and in the area of transfer of personal data across borders. "Electronic-commerce is changing the contours of law and creating new global legal institutions and norms. In today's world of inter-dependence and international commerce, there is increasing importance attached to the growth of harmonization of international commercial norms and regulations."¹³⁰

The importance in the growth of harmonization of international trade rules and regulations in the area of electronic commerce is well illustrated in the development history of the EU Directive. At the time the Commission of the EU proposed the EU Directive in 1990, most of the fifteen Member States had enacted data protection laws based on the 1981 Council of Europe Convention.¹³¹ However, the level of protection varied from Member State to Member State.¹³² These differences sometimes caused difficulties, such as when one Member State blocked the transfer of data to another Member State on the grounds that the other country did not offer a sufficient level of privacy protection. "This lack of a uniform method has already caused problems throughout the European Community in reaching the goal of uninhibited data flows between member states since some countries have adopted stricter regulations than other

¹²³ See SACHA WUNSCH-VINCENT, *The Internet, Cross-Border Trade in Services, and the GATS: Lessons from US-Gambling*, 5 WORLD TRADE REV. 3, 319-355 (2006), at p.319 n.1.

¹²⁴ Sacha Wunsch-Vincent states, in his article, that "this type of electronic service trade is still a relatively new phenomenon when viewed through the lens of international trade rules." *Id.*, at 319.

¹²⁵ See *id.*, at p.320.

¹²⁶ *Id.*

¹²⁷ *Id.*

¹²⁸ AADITYA MATTOO, et al. eds., DOMESTIC REGULATION AND SERVICE TRADE LIBERALIZATION, Washington D.C., World Bank (2003), Chapter 6, Domestic Regulation and Trade in Telecommunications Services: Experience and Prospects under the GATS, at p.83.

¹²⁹ MAROSS, *supra* note 5, at p.337.

¹³⁰ *Id.*

¹³¹ See SWIRE & LITAN, *supra* note 18, Chapter 2, The Legal Context of the Privacy Directive, pp.22-49, at pp.23-24.

¹³² See *id.*

states.”¹³³ “In effect, these differences became an obstacle to internal unification within the EU.”¹³⁴

What, then, is the effective and desired way to deal with privacy-related issues at the multilateral level, which is both technically and politically feasible for Member countries to genuinely engage in adopting new and enforceable privacy rules? As illustrated above, neither the self-regulatory and sector specific approach taken by the United States or the EU Directive will be sufficient to address effective solution to cross-border trade of personal data. In addition, the principles underlying the APEC Framework do not provide any enforcement mechanism and/or remedial solution to potential privacy-related problems.

As illustrated in the case of Asia Pacific region, many countries are without any privacy legislations, let alone affording an “adequate level of protection” over the transfer and maintenance of personal information across and within countries. The necessary instruments to adopt and execute national privacy legislations are fundamental issue to be resolved by each WTO Member country. Without adequate and effective enforcement measures, compliance with privacy law would have no practical effect. There has to be sufficient legal as well as social infrastructures in a country for privacy legislations to have the full effect.

Furthermore, the legal protection of individual’s privacy is a luxury in some developing countries. This is due to the fact that, in many cases, they first need to address other important aspects in the society, such as corruption, utter disregard for human rights, labor rights and environmental issues. As such, many Member countries may be unwilling to commit to a certain level of privacy protection.

In light of rapidly growing trade in electronic commerce, businesses and multinational companies can help shape certain aspects of standards related to transfer of personal data across borders. “The private sector is leading the way in setting global technological standards for electronic commerce, and it can also help resolve the technical aspects relevant to policymaking concerns in areas ranging from tax administration to privacy protection.”¹³⁵ At the same time, there is, and will continue to be, a critical need for establishing a standardized set of privacy rules with respect to the virtual and electronic transfer of personal data across borders. “Consumer protection is absolutely essential if people are to have confidence that transactions on-line are as safe as those in the physical world.”¹³⁶

If the subject of privacy were to be negotiated at the multilateral level, the proper balance must be maintained between facilitating the flow of trade, having adequate and effective enforcement measures in place and addressing other social objectives such as human rights. Moreover, if new privacy rules within the GATS framework are necessary in order to facilitate the free flow of personal data across border, the GATS framework must provide sufficient guidance to Member countries to adopt and execute privacy rules at the national level.

However, if the existing GATS framework does not provide sufficient guidance for Member countries to deal with the issues related to privacy in electronic commerce, it may be more feasible for Member countries to come to terms with flexible approach to

¹³³ An example of problems is illustrated in the case of Fiat as follows. “For example, the parent company of Fiat, located in France, wanted to transmit employee career data to its subsidiary, in Italy, for use in an internal Human Resource Database. The information was to be transmitted by code, not by name, for statistical purposes. However, the French data was not allowed to be transmitted to Italy because the Italians did not have any Data Protection Laws and had not ratified the European Convention.” KRAUS, *supra* note 51.

¹³⁴ GEORGE, LYNCH, MARSNIK, *supra* note 9, at p.741.

¹³⁵ HOEKMAN, et al. eds., *supra* note 103, Chapter 31, Electronic Commerce, the WTO, and Developing Countries, at p.323.

¹³⁶ SAUVÉ, et al. eds., *supra* note 4, Chapter 14 Global Electronic Commerce and GATS: The Millennium Round and Beyond, pp.399-437, at p.428.

supplementing the existing disciplines under the GATS.¹³⁷ Or even before the sufficiency of the current GATS framework can be analyzed, there is an issue of whether personal data traded over the Internet should fall under the disciplines of the GATT and/or GATS, the issue of which will not be examined in this article.¹³⁸

In the context of application of privacy laws and the potential conflicts arising thereof, the EU Directive, for instance, may clash with free trade agreements between countries in the following ways.

“First, the United States and other non-EU countries may argue that the Directive is an improperly extraterritorial enactment and that it is none of Europe’s business to dictate how personal information should be handled outside Europe. Second, there is a suspicion among some that the Directive may serve protectionist goals, saying “none of your business” to non-European companies that face the barrier of having to comply with complex European privacy laws.”¹³⁹

Moreover, Peter P. Swire and Robert E. Litan (1998) suggest two prospective ways in which privacy-related challenges could be brought under WTO law.

“First, a European data protection law can be challenged by third countries under the WTO trade rules. If the challenge succeeds, diplomatic pressure can be applied to the offending country to change its behavior, and trade sanctions can also be imposed by the country that brought the challenge. Second, privacy laws might become part of WTO negotiations. In this way the WTO might become a useful forum for resolving disagreements about data protection rules. Ultimately, new privacy rules might even be included in treaties that are negotiated through the WTO.”¹⁴⁰

In any case, it is important to find the most appropriate means of establishing the standard privacy rules which incorporates a dispute resolution mechanism. The question, then, becomes one of structuring a format within the GATS framework, i.e., “whether members wish to elaborate a Part III ‘patchwork’ framework of disciplines applicable only through specific commitments or a Part II general framework of disciplines applicable to all members.”¹⁴¹ In this context, we will first address the potential privacy issues arising out of Members’ rights and obligations within the GATS framework and how best to resolve these potential conflicts within the existing rules on trade in services, i.e., whether privacy issues should be addressed through an adoption of the comprehensive, horizontal disciplines as opposed to the sector-specific disciplines.

5.1.1. MFN principle

Domestic privacy law may violate the free trade principles under the WTO rules. The GATS MFN principle is a general obligation applicable to all Members, unless a

¹³⁷ See *id.*, at p.404.

¹³⁸ For example, as the trade and the number of transactions via Internet increase, “[s]ome of the traditional distinctions between domestic and foreign services and in the classification of goods and services begin to blur in the Internet marketplace. HOEKMAN, et al. eds., *supra* note 103, Chapter 31, Electronic Commerce, the WTO, and Developing Countries, at p.316.

In addition, “[the issue of classification of goods traded in digital form, i.e., whether the transaction should fall under the purview of GATT or GATS,] has become a political issue on which governments and international businesses are at times divided. The European Commission argues that all transmissions of digital products constitute services and fall under the scope of GATS.” This “‘all services’ approach ... would ensure that EU policies on privacy protection ... apply to the supply of digital products.” SAUVÉ, et al. eds., *supra* note 4, Chapter 14 Global Electronic Commerce and GATS: The Millennium Round and Beyond, pp.399-437, at p.408.

¹³⁹ SWIRE & LITAN, *supra* note 18, at pp.188-189.

¹⁴⁰ *Id.*, at p.189.

¹⁴¹ MATTOO, et al. eds., *supra* note 128, Chapter 7, GATS Regulatory Disciplines Meet Global Public Goods: The Case of Transportation Services, at p.120.

Member clearly demonstrates its intention to exempt itself from this non-discrimination obligation by specifically listing an inconsistent measure in the Annex on Article II Exemptions.

“The panel report on *EC – Bananas III* confirmed what the legislative distinction between general obligations and specific commitments had already implied, that the MFN obligation applies to all service sectors and suppliers irrespective whether specific commitments have been undertaken.”¹⁴² Applying this general MFN principle to the implementation of privacy legislation, if a Member country with a strict domestic privacy law grants permission for data transfer across borders to one Member, but treats any other Member less favorably by not granting permission for “like” data transfer, the Member implementing the strict privacy legislation might be subject to the WTO dispute in violation of its obligation under Article II of the GATS.

“This situation might arise, for instance, if the European Union permitted transfers to former colonies in the third world, while denying transfers to the United States. If the United States has stricter data protection laws and practices than the former colonies, it might have a strong case in the WTO for violation of the most-favored-nation provision.”¹⁴³

If a member country listed an exemption in its Schedule of Commitments and the list of Article II exemptions, the application of domestic privacy law, which may result in less favorable treatment of a Member compared to other Members (and may constitute a violation of Article II MFN principle), could be justified.

Under the current schedules of commitments and list of Article II exemptions, Australia, EC, Hong Kong, Japan and the United States had not listed any exemption relating to privacy and/or handling and processing of personal data.¹⁴⁴

5.1.2. *Domestic Regulation under Article VI*

One of the objectives to be achieved through the adoption and implementation of privacy legislation is to ensure the quality of services provided to consumers. At the same time, however, the extraterritorial nature of privacy legislation could reach beyond its intended object and purpose and become a major hindrance to trade liberalization. The domestic privacy laws and the application thereof may create barriers to new product and marketing partnerships by restricting the timely exchange of necessary data. With a legitimate policy objective, could a country justify its national privacy legislation based on Article VI of the GATS?

Article VI of GATS provides that “In sectors where specific commitments are undertaken, each Member shall ensure that all measures of general application affecting trade in services are administered in a reasonable, objective and impartial manner.”¹⁴⁵ Article VI of GATS further stipulates that “With a view to ensuring that measures relating to ... licensing requirements do not constitute unnecessary barriers to trade in services, the Council for Trade in Services shall... develop any necessary disciplines.”¹⁴⁶ These disciplines shall ensure that such licensing requirements are “(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: (c)

¹⁴² MATSUSHITA, SCHOENBAUM, MAVROIDIS, *The World Trade Organization, law, practice, and policy*, OXFORD U. PRESS (2006), at p.619.

¹⁴³ SWIRE & LITAN, *supra* note 18, at p.190.

¹⁴⁴ See the list of Article II exemptions for Australia, EC, Hong Kong, Japan and the United States, available at http://www.wto.org/english/tratop_e/serv_e/serv_commitments_e.htm (last visited July 6, 2009).

¹⁴⁵ Article VI:1 of GATS.

¹⁴⁶ Article VI:4 of GATS.

in the case of licensing procedures, not in themselves a restriction on the supply of the service.”¹⁴⁷

In other words, the underlying disciplines of GATS Article VI are both substantive and procedural in nature. The procedural aspect of Article VI is to avoid arbitrary regulation and administration of rules that affect trade in services. The procedural principles of Article VI, therefore, ensure a prohibition of abuse of rights by administering body. On the other hand, the substantive aspect and the underlying objective of Article VI are not to assess the validity or necessity of an adopted measure in question, whose purpose is to achieve a legitimate policy goal. Rather, Article VI aims to assess whether such measure is applied in discriminatory and unreasonable manner.¹⁴⁸ “For the time being, the only relevant work in this field has been undertaken in the context of professional services and, more specifically, in the accountancy sector.”¹⁴⁹

The Disciplines on Domestic Regulation in the Accountancy Sector¹⁵⁰ (the “Disciplines”) were adopted in December 1998. The Disciplines set forth the obligations of the WTO Members, regardless of whether they have undertaken specific commitments in the accountancy sector.¹⁵¹

“The draft disciplines do not focus on the substantive content of qualifications in accountancy but seek to ensure *procedural transparency* in matters of licensing and qualification. One of the most important elements of the disciplines is the creation of a *necessity test*, which requires that measures relating to licensing, technical standards, and qualifications be *no more trade restrictive than necessary* to fulfill a legitimate public policy objective. With regard to standards, for instance, the disciplines require that they be prepared, adopted, or applied *only to fulfill legitimate objectives*, which are stated to include the *protection of consumers, the quality of service...*”¹⁵²

In considering the potential for establishing privacy standards at the multilateral level, the question becomes whether the same (or similar) principles as laid out in the Disciplines could be applied. It is important to note, however, that the Disciplines are designed in a way that they are only applicable to a specific service sector.¹⁵³ Because international transfer (and cross-border trade) of personal data entails business operations in almost all service sectors, an adoption of sector specific disciplines may not be the optimal approach in dealing with privacy related issues within the framework of GATS.¹⁵⁴

¹⁴⁷ Article VI:4(a)-(c) of GATS.

¹⁴⁸ See MATTOO, et al. eds., *supra* note 128, Chapter 11, Regulation on Health Services and International Trade Law, at p.206.

¹⁴⁹ MATSUSHITA, SCHOENBAUM, MAVROIDIS, *supra* note 142, at p.628.

¹⁵⁰ WTO Docs S/L/64 of 17 December 1998.

¹⁵¹ See MATSUSHITA, SCHOENBAUM, MAVROIDIS, *supra* note 142, at p.628.

¹⁵² MATTOO, et al. eds., *supra* note 128, Chapter 1, Domestic Regulation and Trade in Services: Key Issues, at pp.3-4 (emphasis added).

¹⁵³ A sector-specific commitment under the GATS “applies to trade in services in a particular sector.” World Trade Organization, Guidelines for the Scheduling of Specific Commitments under the General Agreement on Trade in Services (GATS), WTO Doc S/L/92, (adopted on March 23, 2001), at p.11.

¹⁵⁴ As a reference, a horizontal commitment “applies to trade in services in all scheduled services sectors unless otherwise specified. It is in effect a binding, either of a measure which constitutes a limitation on market access or national treatment or of a situation in which there are no such limitations.” World Trade Organization, Guidelines for the Scheduling of Specific Commitments under the General Agreement on Trade in Services (GATS), WTO Doc S/L/92, (adopted on March 23, 2001), at p.10.

5.1.3. General Exceptions under Article XIV(c)(ii)

“[A] safeguard for individual privacy is built into the framework of the GATS itself.”¹⁵⁵ The general exception clause under Article XIV provides more leeway to Member countries in adopting and implementing their domestic privacy legislations.

Article XIV(c)(ii) stipulates that:

Subject to the requirement that such measures are not applied in a manner which would constitute *a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services*, nothing in this Agreement shall be construed to prevent the adoption or enforcement by any Member of measures: ... (c) *necessary* to secure compliance with laws or regulations which are not inconsistent with the provisions of this Agreement including those relating to: ... (ii) the protection of the privacy of individuals in relation to the processing and dissemination of personal data and the protection of confidentiality of individual records and accounts. (Emphasis added).

“Like other such exceptions provisions, Article XIV is subject to a safeguard against abuse in that measures taken under it may be challenged by other Members on the ground that they are not necessary, or are more restrictive than necessary, to achieve the stated objective. Nor should they be applied in a manner which constitutes unjustifiable discrimination between Members or a disguised restriction on trade in services.”¹⁵⁶

Further, “[t]he analysis under this provision is [] twofold. First, it is necessary to determine whether the objective of the measure concerned pursues one of the objectives indicated in Article XIV and, second, whether its application is made in good faith.”¹⁵⁷ The question is, therefore, whether the application of national privacy laws, such as the EU Directive, is “necessary to secure compliance” with privacy laws, which are consistent with the provisions of the GATS, and whether such measures constitute “arbitrary or unjustifiable discrimination” or “a disguised restriction on trade in services.”

The analysis under Article XIV of the GATS is similar to the analysis by both the Panel and the Appellate Body in *US – Tuna Dolphin*¹⁵⁸ and *US – Shrimp*¹⁵⁹ cases. In *US – Tuna Dolphin*, the GATT Panel was asked to examine the GATT’s consistency of the US Marine Mammal Protection Act (the “Mammal Protection Act”), which established the dolphin protection standards for both the US domestic fishing fleet and for countries whose fishing boats catch yellow-fin tuna in the Pacific Ocean.

According to the Mammal Protection Act, if a country that exported tuna to the United States could not prove it met the dolphin protection standards under the Mammal Protection Act, the United States would ban all imports of the fish from that particular country. In the dispute, Mexico was the exporting country whose exports of tuna to the United States were banned based on the application of the Mammal Protection Act.

One of the issues the Panel examined was whether the United States was allowed to ban all imports that did not meet the standards established under the US domestic law, i.e., whether the United States could take trade action in order to enforce its own

¹⁵⁵ World Trade Organization, GATS Fact and Fiction, available at http://www.wto.org/english/tratop_e/serv_e/gatsfacts1004_e.pdf (last visited July 6, 2009), at 12.

¹⁵⁶ Note by the Secretariat, The Work Programme on Electronic Commerce, S/C/W/68 (Nov. 16, 1998), para.26.

¹⁵⁷ MATTOO, et al. eds., *supra* note 128, Chapter 11, Regulation on Health Services and International Trade Law, at p.207.

¹⁵⁸ See Report of the Panel, *United States – Restrictions on Imports of Tuna*, DS29/R (June 16, 1994).

¹⁵⁹ See The Appellate Body Report, *United States – Import Prohibition of Certain Shrimp and Shrimp Products*, WT/DS58/AB/R, (adopted on October 12, 1998).

domestic laws in another country and whether the application of the Mammal Protection Act was justified under Article XX(b)¹⁶⁰, (d)¹⁶¹ and (g)¹⁶².

The Panel concluded, *inter alia*, that the United States had not proved that the import ban on tuna from Mexico was “necessary” within the meaning of Article XX(b) i.e., the application of the Mammal Protection Act was the *least-trade restrictive way* to protect dolphins, as opposed to, for example, negotiating dolphin-protection agreements with other countries including Mexico.

It is important to note that the Panel’s holding in *US – Tuna Dolphin* rejected the extraterritorial application of the US domestic law, i.e., the United States could not use Article XX exception(s) to regulate natural resources outside of its borders. The decision of the Panel explicitly limited the right of a country to apply its domestic measures extraterritorially to protect environmental resources.

Seven (7) years after the circulation of the GATT Panel Report on *US – Tuna Dolphin*, the WTO Panel and Appellate Body Reports were adopted in 1998 in the case of *US – Shrimp*. In *US – Shrimp*, the Panel and the Appellate Body examined the application of the US law¹⁶³, which established, *inter alia*, that the imports of shrimp harvested with technology, which may have adverse effect on certain sea turtles, could be banned (unless the harvesting country was *certified* to have a regulatory program and an ‘incidental take-rate’ *comparable to* that of the United States, or the particular fishing environment of the harvesting country did not pose a threat to the certain category of sea turtles).

In its ruling, the Appellate Body examined the WTO consistency of extraterritorial application of the US domestic measure, the aim of which was to protect the environment. The Appellate Body held that the US measure qualified for provisional justification under Article XX(g)¹⁶⁴, but the application of the measure failed to meet the requirements under the chapeau of Article XX, i.e., the US measure was applied in a manner that constituted “a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.”¹⁶⁵ The Appellate Body ruled against the United States, not because the adoption of the measure in question was unjustifiable under Article XX, but because the US measure was applied in a manner inconsistent with the chapeau of Article XX of GATT.

It is important to note that the holding of the Appellate Body implicitly recognized Member countries’ right to take trade action in order to protect the environment *regardless of the extraterritorial nature of the domestic measure*. “As we emphasized in *United States – Gasoline*, WTO Members are free to adopt their own policies aimed at protecting the environment as long as, in so doing, they fulfill their obligations and respect the rights of other Members under the *WTO Agreement*.”¹⁶⁶

Another significance of the holding by the Appellate Body in *US – Shrimp* was its finding of “arbitrary discrimination.” The Appellate Body held that the application of the

¹⁶⁰ Article XX(b) of the GATT allows Members to adopt and enforce measures that are “necessary to protect human, animal or plant life or health” as long as the application thereof would not constitute “a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.”

¹⁶¹ Article XX(d) of the GATT allows Members to adopt and enforce measures that are “necessary to secure compliance with laws or regulations which are not inconsistent with the provisions of [the GATT], ...” as long as the application thereof would not constitute “a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.”

¹⁶² Article XX(g) of the GATT allows Members to adopt and enforce measures that are “relating to the conservation of exhaustible natural resources if such measures are made effective in conjunction with restrictions on domestic production or consumption” as long as the application thereof would not constitute “a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade.”

¹⁶³ Section 609 of Public Law 101-102, codified at 16 U.S.C. 1537 note, amending the Endangered Species Act of 1973, 16 U.S.C. § 1531 *et seq.*

¹⁶⁴ See *US – Shrimp*, *supra* note 159.

¹⁶⁵ *US – Shrimp*, *supra* note 159, at para.186.

¹⁶⁶ *Id.*

US measure in question constituted “arbitrary discrimination” within the meaning of Article XX chapeau, due to its “rigidity and inflexibility.”¹⁶⁷

Applying this “rigidity and inflexibility” reasoning to an analysis of domestic privacy legislations under the GATS framework, the EU Directive, and its application, for example, could be found as “arbitrary discrimination” if it “imposes a single, rigid and unbending requirement”¹⁶⁸ that countries trying to import personal data from the EU adopt privacy laws that afford ‘adequate level of protection’ “without inquiring into the appropriateness of that program for the conditions prevailing in the [importing] countries.”¹⁶⁹

In the absence of WTO case law on this particular issue, it could correctly be argued that “[t]he language in Article XIV(c)(ii) provides a significant legal defense against a claim that the [EU] Directive or national privacy laws violate GATS or the free trade regime more generally.”¹⁷⁰ At the same time, however, if privacy issues were to be negotiated at the multilateral level, which would allow a Member to pay particular attention to the appropriateness of the privacy standards and their general applicability to the conditions prevailing in other Member countries, the problem associated with discriminatory application of domestic measures could be resolved.¹⁷¹

At this point in time, we could correctly assume that the Panel and/or the Appellate Body would rule on the applicability of GATS Article XIV(c)(ii), which would be in line with their analysis of GATT Article XX, i.e., whether the adoption of domestic privacy measures would fall under Article XIV(c)(ii).¹⁷² If such measures fall under Article XIV exception, the question is whether the application thereof constitutes a means of arbitrary or unjustifiable discrimination between countries where like conditions prevail, or a disguised restriction on trade in services.

5.1.4. Market Access under Article XVI

According to Article XVI of the GATS, WTO Members wishing to open their services market to foreign competition indicate, in their Schedule of Commitments, the specific sectors to which they make commitments. Article XVI disciplines the use of quantitative restrictions by prohibiting adoption of six (6) types of measures.¹⁷³

The most recent case on GATS Article XVI, where the electronic delivery of services was involved, is *US – Gambling*¹⁷⁴. In *US – Gambling*, Antigua challenged the

¹⁶⁷ *Id.*, at para.177.

The Appellate Body reasoned that “...Section 609, in its application, imposes a *single, rigid and unbending requirement* that countries applying for certification under Section 609(b)(2)(A) and (B) adopt a comprehensive regulatory program that is *essentially the same* as the United States’ program, *without inquiring into the appropriateness of that program* for the conditions prevailing in the exporting countries.”

¹⁶⁸ *Id.*

¹⁶⁹ *Id.*

¹⁷⁰ SWIRE & LITAN, *supra* note 18, at p.191.

¹⁷¹ Based on the analysis of the Appellate Body in *US – Shrimp*, a WTO inconsistent measure may nevertheless be found to be justified under Article XIV chapeau as long as the application of such measure does not constitute “a means of arbitrary or unjustifiable discrimination between countries where the same conditions prevail, or a disguised restriction on international trade,” i.e., the room for flexibility is provided in the application of a domestic measure (that is aimed to attain a legitimate policy objective) by, for example, negotiating with all interested parties as to how a comparable measure could be adopted in these countries at the domestic level.

¹⁷² This view is supported by the holding of the Appellate Body in *European Communities – Regime for the Importation, Sale and Distribution of Bananas* (hereinafter “*EC – Bananas III*”), where the Appellate Body stated that: “The Panel would have been on safer ground had it compared the MFN obligation in Article II of the GATS with the MFN and MFN-type obligations in the GATT 1994.”, *EC – Bananas III*, WTO Docs WT/DS27/R & WT/DS27/AB/R (September 25, 1997), para. 321.

¹⁷³ The prohibited measures are: (a) limitations on the number of suppliers; (b) limitations on the total value of service transactions or assets; (c) limitations on the total number of natural persons that may be employed; (d) measures which restrict or require specific types of legal entity or joint venture; (f) limitations on the participation of foreign capital. GATS Article XVI:2(a) through (f).

¹⁷⁴ See Report of the Panel, *US – Measures Affecting the Cross-border Supply of Gambling and Betting Services* (hereinafter “*US – Gambling*”), WT/DS285/R (November 10, 2004) and *US – Gambling*, the Appellate Body Report, AB-2005-1, WT/DS285/AB/R (April 7, 2005).

application of US laws, which affected the cross-border supply of Internet gambling services. The Appellate Body upheld the Panel's finding that the United States acted inconsistently with Articles XVI:1 and XVI:2 by prohibiting the cross-border supply of gambling and betting services, *where specific commitments had been undertaken*.¹⁷⁵ This inconsistency amounted to a "zero quota" that fell within the scope of, and was prohibited by, Articles XVI:2(a)¹⁷⁶ and XVI:2(c)¹⁷⁷.

Furthermore, "[g]iven the logic of the underlying WTO ruling on intra-modal technological neutrality [], a total prohibition of the electronic delivery of a service is identical to a significant market access limitation."¹⁷⁸ Therefore, regardless of different technological means of delivering services across borders, i.e., over the Internet, postal services and/or telecommunications, the WTO jurisprudence seems to prohibit, under market access disciplines of Article XVI, Members from applying 'qualitative restrictive' measures that would amount to 'total prohibition' (therefore 'zero quota') of services being supplied across borders.

In the context of privacy legislations, the EU Directive, for example, imposes other WTO Members certain privacy standards (regardless of its legitimate policy objective to ensure the quality of service provided to consumers by maintaining 'adequate level of protection'). Such requirement to maintain 'adequate level of protection' could be found to be so stringent, as applied to particular country(ies), whose existing internal conditions do not allow them to adopt the compatible privacy laws, that it amounts to be a total prohibition on the supply of services (e.g., data processing services outside of the EU Member States).¹⁷⁹ If so found, there would be a strong possibility for the EU Directive to fall within the purview of Article XVI of the GATS, i.e., the EU Directive violates the obligations under Article XVI.

At the same time, however, Article XVI has its limitations. A Member country's obligations under Article XVI extend only to the specific commitments undertaken by that Member. In other words, the obligations under Article XVI do not apply to Members in the absence of specific market access commitments undertaken by them. In this case, Members are free to adopt, and impose upon other Members, any standards that would otherwise be considered as protectionist measures with (intended or unintended) effect of restricting the flow of trade in services.

5.1.5. National Treatment principle under Article XVII

Article XVII of GATS provides for another non-discrimination principle by requiring all Members to accord treatment no less favorable to foreign services and service suppliers than the treatment accorded to their "own like services and service suppliers"¹⁸⁰ *only if* a Member explicitly demonstrates its intention to provide national treatment to foreign services and service suppliers in certain sectors, by inscribing them in its Schedule of Commitments. The following example will illustrate what may happen to the activities regulated under the EU Directive, if the EC binds itself (and such

¹⁷⁵ See Report of the Appellate Body, *US – Gambling*, AB-2005-1, WT/DS285/AB/R (April 7, 2005), at para.265 (emphasis added).

¹⁷⁶ See *id.*, at paras.237-238.

¹⁷⁷ See *id.*, at para.252.

¹⁷⁸ WUNSCH-VINCENT, *supra* note 123, at p.341.

In his article, the author explains the concept of "intra-modal technological neutrality" as follows: "In the context of GATS market access ... obligations, the question was raised whether specific commitments for GATS mode 1 encompass the delivery of services through electronic means...the answer should be yes." Reference is made to WT/GC/16 (February 12, 1999).

The author further elaborates that "[t]his underlies the idea that in no area of the WTO are there different rules for different techniques of delivery." Reference is made to S/C/8 (March 31, 1999).

¹⁷⁹ Even in the case of Australia, where the comprehensive privacy legislation (the Federal Privacy Act of 1988) exists, it is not considered to afford 'adequate level of protection.' See Australian Government, *supra* note 77, at p.3.

¹⁸⁰ Article XVII:1 of GATS.

activities) with the principle of national treatment in its Schedule of Specific Commitments.

For example, the EU Directive may be found to accord less favorable treatment to a service supplier situated in a non-EU country, which is also a WTO Member, than the treatment accorded to a like supplier in one of the EU Member States. A foreign data controller in the UK may be prohibited from transferring personal data to its subsidiary data processor in India, where no privacy law currently exists. This situation may give rise to more favorable treatment to another UK data controller, who collects and handles the same type of consumer data and whose subsidiary data processor is located in one of the WTO Member countries that satisfies the EU's 'adequacy' findings.

In addition, paragraphs 2 and 3 of Article XVII of GATS stipulate that: "A Member may meet the requirement of paragraph 1 by according ... either formally identical treatment or formally different treatment[, which] shall be considered to be less favourable *if it modifies the conditions of competition* in favor of services or service suppliers of the Member compared to like services or service suppliers of any other Member."¹⁸¹ Therefore, the question is how the competitive conditions in a particular market are affected by the application of domestic privacy laws. Article XVII of GATS explicitly incorporates the *de facto* discrimination doctrine developed in GATT context. The *de facto* discrimination doctrine provides that it may not be sufficient for a Member's measure to accord the same regulatory treatment. What matters is whether equal competitive conditions are being provided. The doctrine ensures, in other words, that a Member will not be able to do indirectly what it is not allowed to do directly under the national treatment principle.

In *EC – Bananas III (Article 21.5)*¹⁸², the measure adopted by the EC regulated the imports of bananas into the European Communities and access to the EC market for three (3) different categories of bananas. The Panel, after examining the application of the EC measure, concluded that Ecuador's suppliers of wholesale services were *de facto* granted less favourable treatment than suppliers of the EC and Africa, Caribbean and Pacific ("ACP") countries, in violation of GATS Article XVII. The Panel also found that the requirements for the EC's licensing schemes violated Article XVII, since the requirements resulted in *de facto* less favourable conditions of competition accorded to Ecuador in the EC market than accorded to like service suppliers of the EC.

It follows, therefore, that if the EU Directive and the application thereof accords less favorable treatment to foreign data processor (in the example above), it could be considered as *de facto* discrimination against that foreign service supplier, in favor of the domestic data processor in one of the EU Member States. In the absence of specific commitment by the EC in its Schedule of Commitments (under national treatment column), there is a potential for such challenge by other Members and the resulting finding by the Panel and/or the Appellate Body.

Again, however, the principle of national treatment is *only applicable* where a Member commits itself to afford the equal treatment to certain sectors by inscribing them in its Schedule of Specific Commitments. As in other Article(s) under the GATS, this gives much leeway for Member countries to adopt their national legislations and apply them in ways they see fit, regardless of their effect to (and sometimes against) competitions from abroad.

¹⁸¹ Article XVII:2 and 3 of GATS (emphasis added).

¹⁸² Report of the Panel, *European Communities – Regime for the Importation, Sale and Distribution of Bananas – Recourse to Article 21.5 of the DSU by Ecuador*, WT/DS27/RW/ECU (circulated on April 12, 1999).

5.1.6. *International Standard on Transfer of Personal Data*

Aside from applying the GATS disciplines to personal data transfer across borders, the creation of international privacy standard will undoubtedly facilitate the flow of trade in services. The approach taken in the financial services sector is a good example of setting international standards at the multilateral level. “The approach to financial services regulation is increasingly based on the compliance of domestic financial systems with internationally formulated norms... In some sense the financial sector perhaps more than other sectors has recently been subject to harmonization through a number of globally formulated standards.”¹⁸³

In addition, the International Organization for Standardization (“ISO”) has adopted guidelines on data protection to facilitate trans-border flows of personal health information (hereinafter “ISO Guidelines”).¹⁸⁴ The ISO standards provide, at the global level, directional guidance to governmental authorities and private companies when they implement and adopt their national and/or industrial rules and principles.

The ISO Guidelines “aim[] to facilitate international health-related applications involving the transfer of personal health data. It seeks to provide the means by which data subjects, such as patients, may be assured that health data relating to them will be adequately protected when sent to, and processed in, another country.”¹⁸⁵ However, the ISO standards are only directional tool to be consulted by countries and these standards do not provide legal advice or any remedial/enforcement measures in case of default.

Therefore, “[e]xtending [the responsibility of monitoring the quality of services to and raising the awareness of the risks associated with financial services among] consumers and investors require[] standards in areas such as fraud, privacy, and transparency.”¹⁸⁶ Setting the uniform privacy standards at the multilateral level with detailed technical requirements, enforcement and remedial measures would undoubtedly provide better guidance to countries in the areas of cross-border transfer of personal data.

5.1.7. *Decision by the Council on Trade in Services – Annex and Reference Paper*

In addition to the basic disciplines under Article II (MFN), Article VI (Domestic Regulation), Article XVI (Market Access) and Article XVII (National Treatment) that are designed to facilitate trade liberalization, “GATS Article XVIII provides a means for countries to negotiate additional commitments not covered by the basic GATS framework.”¹⁸⁷

For example, the Agreement on Basic Telecommunications¹⁸⁸ led to the adoption of a reference paper. Reference paper is a common set of pro-competitive regulatory principles to which a Member country commits itself by becoming a party to the agreement and incorporating specific commitments in its Schedule of Commitments as additional commitments. “WTO Members were free to include [a reference paper on the

¹⁸³ MATTOO, et al. eds., *supra* note 128, Chapter 8, Regulatory Reform and Trade Liberalization in Financial Services, at p.134.

¹⁸⁴ International Organization for Standardization, ISO 22857:2004, Health informatics – Guidelines on data protection to facilitate trans-border flows of personal health information (Mar. 17, 2004).

¹⁸⁵ *Id.*, Abstract, available at http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=36522 (last visited July 6, 2009).

¹⁸⁶ MATTOO, et al. eds., *supra* note 128, Chapter 8, Regulatory Reform and Trade Liberalization in Financial Services, at p.135.

¹⁸⁷ MATTOO, et al. eds., *supra* note 128, Chapter 10, Strengthening WTO Member Commitments in Energy Services: Problems and Prospects, at p.177.

¹⁸⁸ The Agreement on Basic Telecommunications was concluded in February 1997 and implemented in February 1998. The Agreement on Basic Telecommunications is an *annex* to the Fourth Protocol of the GATS and it improves market access for telecommunications service suppliers.

Agreement on Basic Telecommunications], in whole or in part, as *legally binding additional commitments* in their schedules.”¹⁸⁹

In a legal sense, the annex is “an integral part of the GATS,”¹⁹⁰ which means that all WTO Members are legally subject to the obligations inscribed in the annex.¹⁹¹ With respect to the specific commitments on telecommunications, Matsushita, Schoenbaum and Mavroidis (2006) explain the horizontal nature of scheduled commitments in the annex as follows.

“By virtue of the *Annex*, Members must ensure that *all service suppliers* seeking to take advantage of scheduled commitments will be accorded access to and use of public basic telecommunications, both networks and services, on a *reasonable* and *non-discriminatory* basis. It is important to note that Members incur these obligations, irrespective whether they have entered specific commitments in telecoms.”¹⁹²

On the other hand, “[t]he legal nature of the Reference Paper is more complex.”¹⁹³ Members have a choice as to whether to be bound by the new disciplines in additional commitment sections of the Reference Paper. Members may opt to adopt, whole or in part, the negotiated provisions in the Reference Paper when they incorporate these provisions into their domestic law.¹⁹⁴

Furthermore, with respect to establishing negotiating guidelines and procedures for each round of negotiations, the Council for Trade in Services is charged with conducting an assessment of trade in services “in overall terms and on a sectoral basis with reference to the objectives of the [GATS].”¹⁹⁵ “The ongoing GATS negotiations afford the opportunity to reexamine issues that may have been inadequately addressed in the annex and Reference Paper and to address new challenges that were unanticipated or left unresolved during the previous negotiations.”¹⁹⁶

As briefly noted above, when countries negotiate on how best to approach and adopt new rules, such as incorporating privacy rules into the framework of GATS, special consideration must be given to the lack, and/or insufficiency, of adequate legal, societal and administrative infrastructure in developing countries. The issue of negotiating method, therefore, becomes an important element in improving the current GATS regime. “[The issue of negotiating method] grows out of the synergies between the elements of e-commerce readiness.”¹⁹⁷

Due to the special consideration for these synergies, “country delegations will begin emphasizing the ‘horizontal’ approach to negotiations on electronic commerce.”¹⁹⁸ In the horizontal approach, the commitments and obligations inscribed under the GATS would be applied across the board to all service sectors covered by the GATS.

In the world of electronic commerce, where a massive amount of personal data is exchanged between countries every day, regardless of the type of businesses involved,

¹⁸⁹ MATTOO, et al. eds., *supra* note 128, Chapter 1, Domestic Regulation and Trade in Services: Key Issues, at p.4 (emphasis added).

¹⁹⁰ MATSUSHITA, SCHOENBAUM, MAVROIDIS, *supra* note 142, at p.678.

¹⁹¹ Based on how annexes are designed, all WTO Members could be required to apply the provisions in the annex to all of their scheduled commitments horizontally. However, an annex could be designed so as to be sector-specific. It could also be designed as mode-specific, so that the provisions in the annex could be applied horizontally across all sectors.

¹⁹² MATSUSHITA, SCHOENBAUM, MAVROIDIS, *supra* note 142, at p.679 (first emphasis added).

¹⁹³ *Id.*, at p.678.

¹⁹⁴ “To the extent that [the Reference Paper] is adopted [in the National Reference Paper as part of domestic legislation, the] National Reference Paper [becomes] part of the commitments of a given WTO Member.” *Id.*, at p.679.

¹⁹⁵ Article XIX:3 of GATS.

¹⁹⁶ MATTOO, et al. eds., *supra* note 128, Chapter 6, Domestic Regulation and Trade in Telecommunications Services: Experience and Prospects under the GATS, at p.84.

¹⁹⁷ HOEKMAN, et al. eds., *supra* note 103, Chapter 31, Electronic Commerce, the WTO, and Developing Countries, at p.323.

¹⁹⁸ *Id.*

the horizontal approach appears to be the most efficient and natural means to attain the objectives sought under the principles of privacy legislations. Therefore, establishing the new privacy provisions to be incorporated as an integral part of the GATS might best be pursued in a new instrument such as an annex.

6. Conclusion

The author in U.S. Multinational Employers concludes its analysis on the adoption of the EU Directive and its impact on the business operations of multinational corporations by stating that “[t]he overall lesson that multinational employers and those engaged in international business transactions may learn from the current data protection controversy with the EU is that an increasingly integrated Europe brings with it the specter of an increasing intrusion in U.S. business policies.”¹⁹⁹

Is the enactment and application of the EU Directive, however, necessarily an “intrusion,” or is it rather a “chance” for those multinational corporations to revisit their business practices in compiling, maintaining and using the personal information to, for example, improve the information asymmetry between their consumers/employees and themselves?

Balancing between excessive protection of collected personal information and no protection is the fundamental point on which all private entities must focus when shaping their data protection management. This balancing requires careful examination of their existing data protection practice, if any is already implemented, and the necessary changes must be incorporated in accordance with the national, as well as the international privacy framework.

As in any other issues associated with the adoption and application of WTO Member countries’ measures that may have significant effect upon both trade in goods and services, e.g., IP law, competition law and environmental law, balancing the costs and benefits becomes one of the key elements. Whether the issue of privacy, and how the international community as a whole should respond to the rapidly growing virtual world of electronic commerce, will be addressed and negotiated at the multilateral level, i.e., by the WTO Member countries within the framework of the GATS, remains to be seen.

¹⁹⁹ GEORGE, LYNCH, MARSNIK, *supra* note 9, at p.783.