A COMPARATIVE STUDY OF THE APEC PRIVACY FRAMEWORK

A new voice in the data protection dialogue?

Candidate number: 8007

Supervisor: Dr L.A Bygrave

Deadline for submission: September 1, 2006

Number of words: 13,468

(Max. 18.000 – juridical thesis. Max. 22.000 – non-juridical theses)

Date of submission: August 31 2006 (month/date/year)

Content

1 Synopsis

1.1 Introduction

Countries around the world are shifting invariably toward information-based societies. The way we work, interact and enjoy our leisure time has changed dramatically since the emergence of the Internet. Both private and public sectors are increasingly offering services over the Internet, be it e-commerce or e-government services, that require collection of an individual's information on a scale that has thus been unprecedented. The increasing interconnection of the world economies further exacerbates this phenomenon. For example it is perfectly normal for a German citizen living in Japan to buy a book from the US Amazon website and for US Amazon to share his information internally with its Japan branch or with its related suppliers and agents.

The burning questions are how can personal data be processed in a fair and secure manner in one's home jurisdiction and also whenever one's personal data is transferred to other countries? As the above example shows, the concept of 'home jurisdiction' can sometimes be blurred which also highlights the urgent need to have an internationally acceptable standard of protecting personal data.

The need to protect personal data and the rationales for doing so are not new, they have been the topics of discussion since the 1960s.

The European countries were the first to start enacting comprehensive legislation. This caused fears in an increasingly interconnected global economy that European countries with 'higher' standards of data protection would enact 'borders' and prevent the flow of information to other countries which did not have equivalent standards of data protection.

Accordingly, work commenced on international conventions, the result of which was that the international community agreed that protecting personal data was necessary for the safeguarding of an individual's privacy[1]. A common set of core principles emerged and was adopted into various international instruments[2]. The debate however continued (and to this day still continues) on which regulatory model best translates these core principles into practice.

Europe has continued to take the lead in this debate by using human rights law to extend the scope of the core principles. The European Union (EU) in particular requires its Member States to enact data protection legislation overseen by a supervisory authority through the implementation of EC Directive 95/46/EC ("the Directive').

This comprehensive European model has influenced non-European jurisdictions' legislative approaches. A large part of the impetus is arguably due to Article 25 of the Directive that imposes 'adequacy' requirements before permitting transborder flow of data from a EU member state to a non-EU member state. This has resulted in the 'trading up' of data protection standards in non-European countries. For instance, Argentina enacted legislation in 2000 modelled on the Directive[3]. Canada also enacted legislation in 2001 that ensures comprehensive data protection for the private sector[4]. The European Commission has formally ruled that these two countries have satisfied

---

[1] See preamble of the Council of Europe-1981 CoE Convention and the OECD Guidelines 1980. As for what 'privacy' actually means, there is unfortunately no definitive definition. In brief, a few definitions have been proposed such as 'the right to informational self determination', 'the right to be let alone', 'the right of limited accessibility' and privacy related only to one's 'intimate sphere'- See Chapter 7-8, *Bygrave* (2002)

[2] OECD Guidelines 1980, 1981 CoE Convention, UN 1990 Guidelines. See section 2.3.3 for further discussion.

[3] Law for the Protection of Personal Data of 2000,available at http://www.privacyinternational.org/countries/argentina/argentine-dpa.html

[4] See Personal Information Protection and Electronic Documents Act of 2000 (PIPED). Available at http://laws.justice.gc.ca/en/P-8.6/index.html Canada had existing federal legislation that governed public bodies; see Privacy Act which came into effect on July 1, 1983 available at http://laws.justice.gc.ca/en/P-21/index.html.

the 'adequacy' criterion of the Directive[5]. Australia has also enacted amendments to the Privacy Act (1998) by way of the Privacy Amendment (Private Sector) Act 2000 (Cth) which took effect in December 2001 (a year later for some small businesses)[6]. The law puts in place National Privacy Principles (NPPs) based on the National Principles for Fair Handling of Personal Information originally developed by the Federal Privacy Commissioner in 1998 as a self-regulatory substitute for legislation. However, the EU Commission to date has not reached a formal decision on whether Australia has satisfied the 'adequacy' requirement.

More recently, the Asia-Pacific Economic Cooperation Privacy Framework 2004 ("APEC Privacy Framework") which establishes a set of common data privacy principles for jurisdictions in the Asia Pacific region has taken a markedly different position. While it has chosen the OECD Guidelines 1980 as a starting point, its main emphasis is not on the right of privacy *per se* but on the importance of global commerce and the free flow of information. The APEC Privacy Framework is also non-prescriptive with regards to the implementation by its Member Economies. The APEC Privacy Framework has been criticized as being "OECD-Lite"[7].

Is the APEC Privacy Framework a weak instrument and if so why? Does the APEC Privacy Framework's approach negate the international harmonization sparked off by the EU model? Does this mean that data protection standards are going to be 'traded down'?

This paper will seek to answer the aforementioned questions.

---

[5] See Commission Decision C(2003) 1731 of 30 June 2003 - OJ L 168, 5.7.2003 (Argentina) and Commission Decision of 2002/2/EC of 20.12.2001(Canada). The Commission decision is only with regards to Canada's PIPED Act. The Canadian Act and the Commission Decision do not cover personal data held by public bodies, both at federal and provincial level, or personal data held by private organisations and used for non-commercial purposes.

[6] Legislation generally available at http://www.privacy.gov.au/act/index.html

[7] See The APEC privacy initiative: "OECD Lite" for the Asia Pacific, Graham Greenleaf, available at www.bakercyberlawcentre.org

1.2 Organization

Section 2 will examine the EU model of data protection by reviewing:

(i) The underlying values that the legislation seeks to serve;

(ii) The principles set out in the Directive and how these differ from the earlier instruments; and

(iii) The strengths and the weaknesses of the EU model.

Section 3 will examine the APEC Privacy Framework using the same methodology as in Section 2. It will conclude by reviewing the weaknesses of using the comparative method to analyse the EU model and APEC Privacy Framework. Are these two completely different international instruments; is this a case of comparing apples and oranges?

Section 4 will discuss the impact of the APEC Privacy Framework on its Member Economies to assess whether or not there has been, or is likely to be, a 'trading down' of standards.

Section 5 This section will offer thoughts on the future of the APEC Privacy Framework and its role in the field of international data protection legislation.

2 The EU Model

2.1 The Players

The EU currently comprises of 25 Member States[8], many of whom wield significant economic power in their own right. Taken as a single trading bloc, the EU which is home to nearly half a billion consumers is a formidable force to be reckoned with.

Europe has had a long legislative experience in enacting data protection legislation. At a national level, Sweden was the first country in the world to enact data protection laws in 1973. West Germany, Denmark, Austria, France, Norway and Luxemburg followed suit in the late1970s. However, there were also countries such as the United Kingdom, sceptical of the concept of a 'privacy right', that did not appear to have any immediate plans to legislate on this area of the law.[9]

At a pan-European level, the European countries realized that diverging standards (or lack of) data protection laws among member states could adversely affect the free flow of information.

In the 1970s, the Council of Europe, a pan-European intergovernmental organization, began work on what would eventually become the 1981 CoE Convention[10]. Countries outside of Europe soon became concerned about the potential of data protection laws impacting upon international trade and also started work on the drafting of the OECD Guidelines.

---

[8] Member States are: Austria, Belgium, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Slovakia, Slovenia, Spain, Sweden and the United Kingdom

[9] In fact, the United Kingdom only enacted its Data Protection Act in 1984 pursuant to its obligations under the CoE Convention.

[10] The treaty was adopted in 1980 and was opened for ratification on January 1981.

Before the paper examines the various international data protection instruments that emerged, it is illustrative at this juncture to examine what prompted countries to legislate the processing of personal data.

2.2 Rationales for protecting the processing of personal data

The catalysts of and the values behind data protection legislation are varied and complex and a detailed examination is beyond the scope of this paper[11]. However, there is international consensus that data protection laws are necessary to protect an individual's right to privacy[12].

Broadly speaking, the catalysts for data protection legislation can be categorized in the following manner, (i) technological and organisational developments (ii) public fears about these developments and (iii) the nature of other legal rules which form the normative basis for such laws.

It is arguably the third category of catalysts that shapes the legislative response to the first and second categories. Without a compelling normative basis, it is difficult for a society to articulate what is actually at stake and there is little incentive for the legislature to act and address the problem.

This is illustrated by the European experience. In the wake of the atrocities of World War II, fundamental human rights were enshrined in the Universal Declaration of Human Rights adopted by the United Nations in 1948; in particular, the right to a private and family life was specifically recognized in Article 12. Europe having had first hand experience of the traumas of war went on in 1950 to adopt the Convention for the Protection of Rights and Fundamental Freedoms, Article 8 similarly protected the

[11] See Bygrave 2002, Chapters 6-8 for a more detailed discussion.
[12] Supra 1

right to private life. The right to private life is also protected under Article 17 of the International Convention on Civil and Political Rights adopted in 1966.

Some European countries also had values such as human dignity, personality and privacy entrenched in their Constitutions. For instance in Sweden, Section 2 of the Instrument of Government Act of 1974 which is a Constitutional document provides for the protection of individual privacy. Section 3 of the same chapter also provides for a right to protection of personal integrity in relation to automatic data processing. The Danish Constitution of 1953 contains two provisions relating to privacy and data protection while Section 71 provides for the inviolability of personal liberty. In Germany, the right of informational self-determination set out in Article 1(1) and 2(1) of the Federal Republic's Basic Law declares that personal rights (*Persönlichkeitsrecht*) to freedom are inviolable[13].

It is likely that European countries were the first to respond to the threat that automatic data processing poses to privacy because of these international and domestic obligations coupled with public sentiment that backed the protection of human rights after World War II.

How did Europe go about enacting data protection legislation? Academics have identified three main waves of legislative activity[14]. The first wave of legislative activity which took place in Europe in the early 1970s was a response to the emergence of computers and the rise of automated information processing by governments and the business sector. The concern at that time was to counter the centralization of large-scale data banks which were perceived as a threat to the individual's right to private life. Countries like Sweden, Germany and Austria established regulatory bodies to oversee computer and data processing and required that such activities were subject to registration and licensing.

---

[13] See the respective country reports at http://www.privacyinternational.org/survey

The second wave occurred in the late 1970s. The fears of a Big Brother centralized 'data-bank society' were replaced as governments and businesses' data processing capabilities became decentralized. Instead of a means to regulate technology, the protection of a citizen's privacy rights became the focus of legislative activity and in countries such as France, Norway, Denmark, commissions oriented their tasks towards helping citizens to exercise their rights.

The third wave signalled a shift towards a more participatory phase where the right to informational self determination was emphasized. The individual's rights to access personal data that was held by organizations were strengthened and laws were amended for instance granting the right to compensation to the individual whose rights were breached.

This approach of limiting data movement on human rights grounds in turn sparked off different fears in the form of economic concerns such as the fettering of trade. This gave rise to the development of standards for the use and dissemination of personal data or data protection standards which sought to balance the competing interests at stake.

2.3 The Directive- a comprehensive data protection regime and more

In order to fully appreciate the comprehensive nature of the Directive and its influence on the issue of transborder flows of personal data, it is necessary to briefly review the other international instruments that pre-dated the Directive, namely the 1981 CoE Convention and the OECD Guidelines.

Section 2.3.1 and 2.3.2 will review the objective of the respective instrument, its principles and its position on transborder flows of personal data.

---

[14] See Bennett & Raab (2003), Chapter 5, pp 101-104

2.3.1 The 1981 CoE Convention

The preamble highlights the Council of Europe's concern to ensure that the increase of automatic processing did not negatively impact on an individual's rights and fundamental freedoms in particular the right to privacy. At the same time, the Council recognized that 'it is necessary to reconcile the fundamental values of the respect for privacy and the free flow of information between peoples.'

The basic principles set out in the Convention are:

(i) fair and lawful obtaining and processing of personal data
(ii) storage of data only for specified purposes
(iii) personal data should not be used in ways incompatible with those specified purposes
(iv) personal data should be adequate, relevant and not excessive in relation to the purposes to which the data are stored
(v) personal data should be accurate and where necessary kept up to date
(vi) personal data should be preserved in identifiable form for no longer than necessary
(vii) Special categories of data may not be processed automatically unless domestic law provides appropriate safeguards
(viii) there should be adequate security for personal data
(ix) personal data should be available to be accessed by individuals who have rights of rectification and erasure

Apart from the principles relating to the special category of sensitive data and the storage of personal data for no longer than necessary, the other principles are fairly uncontroversial and have been accepted and echoed in latter international instruments.

On the issue of transborder data flows, Article 12(3) provided that member states can prohibit or subject transborder flows of personal data if the other party does not provide an 'equivalent protection'.

However, the effect of the 1981 Convention as a means to regulate the international flow of personal data was fairly limited. It is important to note that the Convention is not a self-executing instrument; in this case Member States have to first sign and then ratify the treaty for it to have any force. Secondly, the Council of Europe does not have a legal structure to ensure proper enforcement of the Convention. This means that ratification per se did not equate a common minimum standard of data protection. Thirdly, the question of data transfers to non-contracting states was left to national law, see Article 12. This had the effect of undermining the mutual confidence amongst ratifiers of the Convention because 'If country A transfers data to country B, the fact that both are parties to the Convention doesn't help if country B is free to allow a further transfer to country C which has no data protection law'[15].

However, this problem was rectified subsequently. In 2001, the Council adopted an additional protocol, the "Additional Protocol to the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data regarding supervisory authorities and transborder data flows"[16]. Article 1 establishes the function of supervisory authorities in each Member country and Article 2 deals with transborder flows of personal data to a recipient which is not subject to the jurisdiction of a Party to the Convention. It establishes the requirement of 'adequacy'.

The Convention also remains relevant in serving as a template for newly democratising European states that are relatively new to data protection legislation.[17] For instance Albania, Bosnia and Herzegovina signed and ratified the Convention in 2004, Serbia and Ukraine, Montenegro in 2005 and the former Yugoslav Republic of Macedonia in 2006.

---

[15] Bainbridge, 1996, p10
[16] Available at http://conventions.coe.int/Treaty/en/Treaties/Html/181.htm
[17] See Treaty Office at http://conventions.coe.int

2.3.2 OECD Guidelines

The OECD is an international organisation which has 30 Member States including the founding Western European countries, the North American countries (Canada, the United States) and Mexico, Japan and Australian and Mexico.

Bennett & Raab describes the OECD as the arena in which the first transatlantic conflicts over privacy protection took place[18]. The conflict boiled down to the American view that information flow should rarely be impeded and the suspicion that the Europeans were in fact using data protection concerns to cover an ulterior trade-protectionist motivation. The Europeans on the other hand viewed the American position as a means to protect US domination in the global marketplace.

This struggle is reflected in the preface that highlights the differing attitudes towards privacy and the need to reconcile 'fundamental but competing values such as privacy and the free flow of information' so as to 'advance the free flow of information between Member countries and to avoid the creation of unjustified obstacles to the development of economic and social relations among Member countries'.

Despite the aforementioned struggle between competing interests, the principles in OECD Guidelines do not differ dramatically from the CoE convention. They are: Collection Limitation, Data Quality, Purpose Specification, Use Limitation, Security Safeguards, Openness, Individual Participation and Accountability. This was partly due to the close contact that the OECD Expert Group maintained with the corresponding organ of the Council of Europe[19].

---

[18]See Bennett & Raab, Chapter 4, pp74-77

[19] See paragraph 20-21 of the Explanatory Memorandum of the OECD Guidelines available at http://www.oecd.org/document/18/0,2340,en_2649_34255_1815186_1_1_1_1,00.html and paragraph 14-16 of the Explanatory Report to the CoE Convention available at http://conventions.coe.int/Treaty/en/Reports/Html/108.htm

The OECD Guidelines does not make any distinction between normal data and sensitive data unlike the CoE Convention. The Committee reached the conclusion that it was probably not possible to identify a set of data which is universally regarded as being 'sensitive' due to different cultural values[20]. The principle of "Openness" was also introduced as a prerequisite for the Individual Participation Principle, the rationale being that 'for the latter principle to be effective, it must be possible in practice to acquire information about the collection, storage or use of personal data'. Such means must also be 'readily available' so that individuals are able to obtain the information without unreasonable cost[21].

There are also 2 major differences between the instruments. Firstly, the OECD Guidelines was voluntary and did not impose any penalties for non-adoption or non-compliance whereas the CoE Convention was legally binding. Secondly, the CoE Convention only applied to automated data processing whereas the Guidelines applied to personal data regardless of the processing medium.

With regards the transborder flow of information, while section 17 of the OECD Guidelines echoes Article 12(3) of the CoE Convention in that Member countries may impose restrictions if the other member country provides no 'equivalent protection', section 18 adds the admonition that Member countries should 'avoid developing laws, policies and practices in the name of the protection of privacy and individual liberties which would create obstacles to transborder flows of personal data that would exceed requirements for such protection."

2.3.3 Core Principles of Data Protection Laws

[20] Supra 19, paragraph 19(a), and 45 of the Explanatory Memorandum of the OECD Guidelines
[21] Ibid, paragraph 56 of the Explanatory Memorandum of the OECD Guidelines

From the provisions of the CoE Convention and the OECD Guidelines, a common set of core principles can be extracted. This has been described as consisting of the following[22]:

(i) Personal information should be collected by fair and lawful means.

(ii) The amount of personal information collected should be limited to what is necessary to achieve the purpose for which the data is gathered and processed.

(iii) Personal information should be collected for specified, lawful or legitimate purpose and not be processed incompatibly from those purposes.

(iv) Secondary use of personal information should occur only with the consent of the person or by authority of the law.

(v) Personal information should be relevant, accurate and complete for the purposes for which it is processed.

(vi) Security measures should be taken to protect personal information.

(vii) Persons should be informed of and given access to information relating to them and to be able to rectify the information if necessary.

(viii) Those responsible for processing information should be accountable for complying with measures giving effect to the above principles.

These principles have been reflected in later instruments such as the Directive and the APEC Privacy Framework. Annex A provides a chart detailing where these principles can be found in the CoE Convention, the OECD Guidelines, the Directive and the APEC Privacy Framework.

2.4 The Devil is in the Details- Strengths and Weaknesses of the EU Model

By the late 1980s, only 17 countries had signed the CoE Convention and only 10 had ratified it. The OECD Guidelines being completely voluntary in nature was seen as a

[22] Bygrave (2002), Chapter 1, p2. See also Chapter 3 for detailed discussion

means ‘to justify self-regulatory approaches rather than as a method to promote good data protection practices throughout the advanced industrial world’[23].

The EU became increasingly concerned that discrepancies in data protection would impede the free flow of personal information throughout the EU and could obstruct the creation of the Internal Market which was due to be completed by 1992. The Commission decided that it was justified in proposing a Directive on the basis of Article 100(a) of the EC Treaty to ensure the establishment and functioning of the Internal Market[24].

The aim of the Directive is to ensure a high level of protection for the privacy of individuals in all member states. Explicit reference is made to the Right of Privacy guaranteed under the European Convention for the Protection of Human Rights and Fundamental Freedoms. Recital 10 states:

> “Whereas the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy, which is recognized both in Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms and in the general principles of Community law; whereas, for that reason, the approximation of those laws must not result in any lessening of the protection they afford but must, on the contrary, seek to ensure a high level of protection in the Community”

Another aim of the Directive is to ensure the free flow of information throughout the Single Market by the harmonization of Member States’ rules[25].

---

[23] Bennett & Raab, Chapter 4, p 77
[24] Bennett & Raab, Chapter 4, p 78
[25] See Recital 8

The general rules of data protection are similar to the information privacy principles found in the OECD Guidelines. The additional principles are the explicit requirements of 'legitimate data processing' in Article 7, the prohibition against processing sensitive data in Article 8, the requirement for providing exemptions for the purposes of freedom of expression in Article 9 and the right of a person not to be subject to a solely automated decision in Article 15.

The Directive and Article 15 in particular is remarkable in that it pre-dated the Internet boom and the full explosive force of the processing of personal information via e-commerce. Article 15 tackles the problem of automated profiling practices and sets out limitations to such practices[26]. While other international instruments do not have an equivalent provision, it has been argued[27] that Article 15 signifies the protection of human integrity and dignity in an ever increasing automated and inhumane world and should be a core principle to counterweigh the increase of automated profiling practices that permeate our lives today.

More importantly, it is the very nature of the Directive that is its greatest strength. The Directive is binding on all Member States[28]. The Directive provides a complete regulatory framework for its Member States to emulate. For instance, the Directive deals with the methods by which the principles are to be enforced in national law in 'Chapter III Judicial Remedies, Liability and sanctions' for instance Article 23(1) states that Member States shall provide any person who has suffered damage as a result of an unlawful processing operation a right to receive compensation from the controller for the damage suffered.

---

[26] Admittedly, there is some ambiguity in the wording of Article 15, see Bygrave (2002) Chapters 18 and 19 for a more detailed discussion.
[27] Supra footnote 23
[28] It is important to note that the Directive does not extend to areas which falls outside the scope of Community law, such as those provided for by Titles V and VI of the Treaty on European Union and in any case to processing operations concerning public security, defence, State security and criminal law. See Article 3 of the Directive.

The Directive also specifies the nature and function of a Member State's supervisory authority, Article 28 states that one or more public authorities are responsible for monitoring the application within its territory of the national provisions adopted pursuant to the Directive. Bennett & Raab observe that the provisions of Article 28 gave supervisory authorities a greater range of powers and responsibilities than had existed within many European data protection regimes[29].

Article 29 and 30 goes on to establish an advisory Working Party from the supervisory authorities in each Member State. The Working Party is expected to give the "commission advice on divergences among national laws and on the level of protection of third countries in respect of Transborder data flows."

Unlike the OECD Guidelines or the CoE Convention which do not require their signatories to impose export restrictions on third countries, the Directive further requires Member States to take measures to prevent any transfer of data to a third country that does not meet the adequacy requirement set out in Article 25 unless exceptions or derogations can be claimed, for instance when the data subject gives his unambiguous consent to the data transfer or when the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the controller and a third party[30].

It is important to highlight that the Directive does not require an 'equivalent' standard of data protection, merely that there be an 'adequate' level of protection. This is to combat the concern that countries may seek to find 'data havens' and thus circumvent the Directive. Article 26(2) defines 'adequate level of protection' as follows:

> 'The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer

[29] Bennett & Raab, Chapter 4, p 80
[30] Examples cited are found in Art 26(1) (a) and (c), the other exceptions are found in Art 26(1)(b),(d)-(f) and Art 26(2).

operation or a set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the county of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in those counties.'

The Working Party established under Article 29 has produced papers to aid in the interpretation of Articles 25 and 26. These are a) Discussion Document: First Orientations on Transfers of Personal Data to Third Countries- Possible Ways Forward in Assessing Adequacy (WP 4)[31], b) Working Document: Judging industry self regulation: when does it make a meaningful contribution to the level of data protection in a third country? (WP 7)[32] and c) Working Document: Transfers of personal data to third countries: Applying Articles 25 & 26 of the EU Data Protection Directive (WP 12)[33]. Of these, WP 12 is the most comprehensive and provides a framework of substantive requirements that a given data protection regime must fulfill in order to achieve the standard of adequacy.

WP 12 suggests any meaningful analysis of 'adequate protection' must involve a) an assessment of the content of the rules applicable and b) an assessment of the means for ensuring their effective application. The content principles are briefly[34]:

(i) the purpose limitation principle

(ii) the data quality and proportionality principle

(iii) the transparency principle

---

[31] Available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1997_en.htm
[32] Ibid
[33] Available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/1998_en.htm
[34] For a more detailed treatment, see Chapter 8 pp 217-230, Jay & Hamilton 2003

(iv) the security principle

(v) the rights of access, rectification and opposition; and

(vi) restrictions on onward transfers

(vii) Special handling of sensitive data

(viii) Possibility to opt out from direct marketing

(ix) Special rules for automated decision making

The enforcement principles are briefly[35]

(i) To deliver a good level of compliance with the rules

(ii) To help data subjects in the exercise of their rights; and

(iii) To provide appropriate redress for the injured party where the rules are not complied with

During the process of making an assessment of adequacy, the Commission will usually consult the Working Party and take into consideration its advice; additionally, it will engage independent expert consultants. The process can be lengthy and complex -- as demonstrated by the assessment of Australia's data protection regime, an assessment which started in 2001[36] and has gone on in fits and starts for almost 6 years and which still has not yet resulted in a formal decision by the Commission.

---

[35] Supra 34

[36] See Working Party Document Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000, available at http://ec.europa.eu/justice_home/fsj/privacy/workinggroup/wpdocs/2001_en.htm

As can be seen, it is quite an involved task be it for the relevant National Data Protection Authority or the Commission to rule on the adequacy of a third country.

It is precisely because the Directive is so comprehensive and all encompassing, that herein also lies the difficulty. Apart from this, the Directive itself is a complex instrument- there are 72 'where-as' in the recital which state the policy intentions behind the Directive. Its principles are also not set out plainly as in the CoE Convention or the OECD Guidelines. This makes it difficult for the average reader to comprehend in what way and how the Directive protects his privacy rights.

In fact, a recent survey carried out in 2003 confirmed this. Amongst the findings were that 68% of EU citizens were not aware of independent authorities that monitored the application of data protection laws, only 32% of EU citizen were aware of their access and rectification rights, only 42% were aware that data processors were obliged to provide information such as their identity and the purpose of such data collection[37].

At a national level, Member States also faced difficulty in transposing the Directive. Although transposition was supposed to be completed by the end of 1998, most Member States only notified implementing measures in 2000 and 2001. Even after transposition, divergences remain even at the most basic level[38].

This is illustrated by the UK case of *Durant v FSA (2003)*[39]. In this case, the applicant was a customer of Barclays Bank. He had unsuccessfully sued the bank previously and wanted to commence litigation against them again. He sought to obtain documents from the FSA which it obtained during its investigation of the bank. The applicant claimed that the documents were personal data and sought access to them under section 7 of the UK Data Protection Act 1998 which implemented the Directive.

---

[37] See Special Eurobarometer 196- Data Protection, Executive Summary p10-11, available at http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm#actions

[38] See generally the 1st report on the implementation of the Data Protection Directive Data Protection Directive 15.05.03, at http://ec.europa.eu/justice_home/fsj/privacy/lawreport/index_en.htm#actions

[39] [2003] EWCA Civ 1746

The UK Court of Appeal however gave a narrow interpretation of the meaning of 'personal data' under s1(1) of the UK Data Protection Act 1998. The Court of Appeal held that the right to access personal data held by another extends only to information about the individual that affects his personal or family life, business or professional capacity.

It has been reported[40] that the European Commission has notified the UK Government that the Data Protection Act 1998 has failed to conform to the Directive and in particular that the definition of 'personal data' adopted by the court adopted in *Durant* was too restrictive. To date, the Commission has not made the enquiry public and it is too early to say how this will all play out[41].

As noted earlier, the Directive contains a groundbreaking requirement set out in Article 25 that prohibits the cross border transfer of data to countries that do not meet the adequacy requirement. It is arguably this particular article that has caused the international community to take heed of the Directive and its implications on their respective domestic legislatures.

However, in the 1st report regarding the implementation[42] of the Directive, the Commission notes that Article 25 and 26 has been implemented in varying fashions. On one hand, some Member States allow the data controller to make the adequacy assessment with very little input from the State or national supervisory authority. On the other hand, some Member States require that all transfers be submitted to the national supervisory authority for authorization despite the exceptions set out in the Directive[43]. The Commission report recognizes that an overly strict approach would create 'a gap between law and practice which is damaging for the credibility of the Directive and for Community law in general.' It concludes the report by calling for the

[40] Usha Jagessar, Vicky Sedgwick (2005)
[41] See *Slow Progress on EU Privacy Programme*, Laura Linkomies, Privacy Laws & Business International Newsletter, Oct/Nov 2004, pp 12-13
[42] Supra 38, see pages 18-19
[43] See Article 26(1) and 26(2) of the Directive

simplification of the conditions for international transfers. It is submitted that this is perhaps the logical way to proceed in light of the enormous amount of data processing that has become part and parcel of the way in which we conduct our daily activities today.

3 The APEC Privacy Framework

3.1 The Players

APEC is an inter-governmental grouping of Pacific Rim economies. Unlike the WTO or other multilateral trade bodies, APEC has no treaty obligations required of its participants neither does it have any formal institutions beyond regular meetings. As such, it is important to bear in mind that decisions made within APEC are reached by consensus and commitments are undertaken on a voluntary basis.

APEC has 21 Member Economies[44] which account for more than a third of the world's population (2.6 billion people), over 50% of world GDP (US$ 19, 254 billion) and in excess of 41% of world trade. APEC also represents the most economically dynamic region in the world having generated nearly 70% of global economic growth in its first 10 years[45].

Member Economies are at different stages in their recognition of privacy rights in their

---

[44] Australia; Brunei Darussalam; Canada; Chile; People's Republic of China; Hong Kong, China; Indonesia; Japan; Republic of Korea; Malaysia; Mexico; New Zealand; Papua New Guinea; Peru; The Republic of the Philippines; The Russian Federation; Singapore; Chinese Taipei; Thailand; United States of America; Viet Nam.

[45] See http://www.apecsec.org.sg/apec/news___media/fact_sheets/about_apec.html

legislatures[46]. The following is not meant to be an exhaustive list but to illustrate the diversity between the Member Economies: Countries like Australia, Canada, Hong Kong, New Zealand, Korea, Taiwan and Japan have legislative regimes that regulate both private and public sectors and apart from Taiwan and Japan have established data privacy agencies. Most countries have segmented legislative coverage, for instance Thailand has data privacy rules covering the government sector, Singapore has opted for a voluntary self-regulatory scheme for the private sector but has not enacted specific data protection legislation for the public sector, the USA has comprehensive legislation for federal agencies but has chosen to enact sector specific legislation for the private sector. Malaysia is in the process of enacting comprehensive data protection laws. Some countries recognize a right to privacy in their constitution but have not enacted general data protection laws like Philippines, Mexico and China.

It is in the context of this diverse background that the APEC Electronic Commerce Steering Group (ECSG) began development of an APEC Privacy Framework in February 2003 at the Data Privacy Workshop in Thailand[47].

3.2 Rationales for protecting the processing of personal data

The impetus for the APEC Privacy Framework is clearly stated in the foreword: "the potential of electronic commerce cannot be realized without government and business cooperation to develop and implement technologies and policies which…address issues including privacy."

The role of the APEC Privacy Framework is to balance and promote effective information privacy protection and the free flow of information in the Asia Pacific region in order to ensure the growth of electronic commerce. This objective is constantly stated in documents leading up to the APEC Privacy Framework. For

[46] For a more comprehensive treatments, see www.privacyinternational.org/survey

instance, in the 16th Ministerial Meeting at the 2004 Santiago Summit, the reaffirmation of the APEC Privacy Framework was clearly in the context of encouraging the emergence of e-commerce[48].

Therefore while the importance of informational privacy is acknowledged, it is in the context of encouraging the growth of e-commerce rather than the need to protect basic human rights and dignities[49]. In fact, the Framework disapproves of regulatory systems that unnecessarily restrict the flow of information as this could adversely impact on global businesses and economies. Instead, APEC recognizes the need to develop new systems 'for protecting information privacy that account for these new realities in the global environment. [50]'

This is arguably not a surprising conclusion. While Europe's experience with history has made it protective of human rights and wary of the way in which technology impacts on these rights, many APEC countries do not share this concern. Instead, many of the APEC countries as described above in section 3.1 do not have a strong legal history of protecting the right to privacy *per se* and are instead rapidly developing countries which are more concerned with the trade opportunities provided by electronic commerce.

Even countries which have existing data protection laws such as USA, Australia and Japan have chosen a market-oriented approach towards data protection which manifests itself in the private or co-regulatory model instead of the existing EU top down regulatory approach. While, the EU does not rule out a "co-regulatory" approach, see

---

[47] Working papers are available at http://www.apec.org/apec/documents_reports/electronic_commerce_steering_group/2003.html

[48] See the Ministerial Statement available at: http://www.apecsec.org.sg/apec/ministerial_statements/annual_ministerial/2004_16th_apec_ministerial.html

[49] See the APEC Privacy Framework, particularly paragraphs 1 and 6 of the preamble, available at http://www.apec.org/etc/medialib/apec_media_library/downloads/taskforce/ecsg/pubs/2005.Par.0001.File.v1.1

[50] Supra 49, see paragraph 8

Article 27 of the Directive, the fact remains that in these countries, gaps remain in its privacy legislation with respect to the regulation of its private sector. For instance, in the case of Australia, the Privacy Amendment (Private Sector) Act does not apply to small businesses that have less than AUD 3 million annual turnover. This is arguably a manifestation of the government's policy choice of preferring businesses over individual rights to privacy. Consequently, this has resulted in data protection laws that diverge from the EU model[51] and thus the European Commission has not formally recognized any of these countries as satisfying the 'adequacy criterion'.

This brings us to the intriguing question of whether the differences in rationales mean a different set of standards.

3.3 The APEC Privacy Framework- A new voice?

There are 9 APEC information privacy principles:

1) Preventing harm
2) Notice
3) Collection Limitation
4) Uses of Personal Information
5) Choice
6) Integrity of Personal Information
7) Security safeguards
8) Access and Correction
9) Accountability

[51] For a more detailed treatment, see pages 341-342, Bygrave (2004)

The APEC Privacy Framework is based on the core values of the OECD Guidelines. It is not surprising that the OECD Guidelines was used as a starting point when one considers that 7 of the APEC member economies are members of the OECD[52].

The main differences are the exclusion of the Openness Principle found in s12 of the OECD Guidelines and the inclusion of the principles of a) Preventing harm and b) Choice in the APEC Privacy Framework.

While the basic principles set out in the APEC Privacy Framework do not differ dramatically from the core principles of the earlier international instruments[53], the APEC Privacy Framework appears rather non-prescriptive with regards to implementation and enforcement and thus has been subject to much criticism[54]. For instance, the domestic implementation guidelines in Part 4 does not require any particular means of implementing the Framework but merely provides that there are several options for giving effect to the Framework 'including legislative, administrative, industry self-regulation' and that the Framework is meant to be implemented in a flexible manner.

No central enforcement body is required only that Member Economies should consider taking steps to establish access points or mechanisms.[55] As for remedies, paragraph 38 states it should include an appropriate array of remedies such as redress and the ability to stop a violation from continuing but does not stipulate that legislative remedies must be put in place.

The above is perhaps an unavoidable consequence as the APEC grouping is a voluntary one and Member Economies are not bound, as the EU member states are, to transpose

---

[52] Australia, Canada, Japan, South Korea, Mexico, New Zealand and USA

[53] See Annex B for a comparative table of the OECD Guidelines, the Directive and the APEC Privacy Framework 2004

[54] See '*Criticisms of the APEC Privacy Principles (Version 9) and recommendations for improvements'*, Baker & Mckenzie Cyberspace Law and Policy Centre, available from www.bakercyberlawcentre.org,

the APEC Privacy Framework into their domestic legislation. However, it is important to note that the APEC Privacy Framework does not prevent Member Economies from having 'higher' standards in recognition that some of its Member Economies already have comprehensive legislation in place.

With regards to cross border data flow, this was an issue that was debated extensively. While the 9 Privacy Principles were announced in November 2004, the original version was silent on the transfer of personal information between APEC economies or to non-APEC countries, Annex 1 to the Framework stipulated 3 areas for future discussion in 2005, they were a) the possibility of sharing information among APEC Member Economies via access points within each Member Economy, b) cross border cooperation between privacy investigation and enforcement agencies and c) the development and recognition of organizations' cross border privacy codes across the APEC region [56].

It was only at the Second APEC Implementation Seminar at Korea in September 2005 that agreement was reached on this missing section and the draft was then forwarded to APEC authorities for formal endorsement. This final version (which incorporated the 3 areas highlighted in Annex 1 of the 2004 draft) was approved in September 2005.

As it stands in its final version[57], the APEC Privacy Framework, unlike the Directive, does not forbid data exports to countries without APEC compliant laws.

The APEC Privacy Framework in fact emphasizes that while it is important to have mechanisms to facilitate responsible and accountable cross-border data transfers and effective privacy protections, Member Economies should endeavor not to create 'unnecessary barriers to cross-border information flows, including unnecessary

---

[55]Supra 49, see in particular paragraphs 31-34

[56] A copy of the document can be accessed at http://www.law.indiana.edu/instruction/fcate/3836/2005/APEC%20Framework%20as%20published.pdf

administrative and bureaucratic burdens for businesses and consumers'[58]. One writer states that this section puts to rest fears that the APEC Privacy Framework was intended to create a data protection bloc which is antagonistic to the EU's adequacy requirements[59].

However, the APEC Privacy Framework differs on 2 aspects which have been covered by previous international agreements. The APEC Privacy Framework does not explicitly allow restrictions on data exports to countries without APEC-compliant laws unlike the CoE Convention and the OECD Guidelines. It also does not require data exports to be allowed to countries that have APEC compliant laws unlike previous international instruments.

Instead, APEC appears to be more interested in the exploration of alternative ways of regulating cross-border transfer of data instead of the traditional top-down regulatory method. This will be examined in more detail in the next section.

3.4 "OECD Lite"? - Strengths and Weaknesses of the APEC Privacy Framework

One of the greatest strengths of the APEC Privacy Framework is that it was drafted squarely in the e-commerce age unlike the Directive which was drafted before the Internet boom. While the APEC Privacy Framework has been criticized as 'having a bias towards [the] free flow of information over privacy protection'[60], it is perhaps an inevitable conclusion when one considers where the APEC economies are coming from. APEC is primarily a forum for trade related interests and of paramount concern would

---

[57] Supra footnote 49, pages 34-36
[58] Ibid, see paragraph 48.
[59] See *APEC Privacy Framework completed: No threat to privacy standards*, Graham Greenleaf, Privacy Laws & Business International Newsletter, Sept/Oct 2005 Issue 79
[60] '*The APEC Privacy Framework- A new low standard'* Graham Greenleaf, Privacy Laws & Business International Newsletter, Jan/Feb 2005 Issue 76,

be how to manage data transfers that are the life blood of global commerce in a manner that respects privacy and yet does not unduly burden organizations.

It is submitted that the APEC Privacy Framework attempts to strike a practical balance which is useful for individuals and businesses. It chooses to focus on aspects of privacy protection that are of most importance to international commerce such as preventing the misuse of personal information rather than broadly protecting the right of privacy per se. This is illustrated in the First Principle of Preventing Harm. The commentary relating to this principle states that one of the primary objectives of the APEC Privacy Framework is to prevent misuse of personal information and consequent harm to individuals and that remedies for such infringements should be **proportionate** to the likelihood and severity of the harm caused. While the choice of establishing this as a principle has been described as 'bizarre'[61], it is respectfully submitted that by starting off with this principle, the APEC Privacy Framework is in fact sending a clear message that it is positioning itself as neutral and balanced. This is in contrast to the high standard that the Directive sets out for its Member States that it deems necessary to protect fundamental human rights such as privacy.[62]

Another interesting principle not found explicitly in the other international instruments is that of the Ninth Principle of Accountability. This principle recognises that business models often require information transfers between different types of organizations in different locations with varying relationships. This imposes duties on the personal information controller such as ensuring that the appropriate consent is given or exercising due diligence to ensure that the recipient person or organization will protect the information consistently with the principles in the APEC Privacy Framework.

This principle has been described as being the most important innovation in the APEC Privacy Framework as it takes the position that 'accountability should follow the data'.

---

[61] Supra footnote 48

That is once an organisation has collected personal information, it remains accountable for the protection of that data despite the fact that it may be passed onto another organisation or jurisdiction.

This means that in the example set out in the Introduction of this paper, that US Amazon would continue to be responsible for the personal data collected from its German customer regardless of whether it uses the personal data internally ie within US or with its Japanese branch or externally with its suppliers whether they are located in US or elsewhere. This is in contrast to other instruments, such as the Directive which focus on controlling the flow of cross border data[63], a concept that may not fit neatly with the way businesses function in our current age.

For instance, one of the recognized exceptions in the Directive for cross border data transfers to countries which do not meet the 'adequacy' requirement is when a controller adduces adequate safeguards for the individual's privacy and fundamental rights. Article 26(2) specifies that such 'safeguards may in particular result from appropriate contractual clauses' [Emphasis added] which the Commission may approve and which Member States would then have to comply with.

Thus, in 2001, the Commission approved two sets of standard contractual clauses [64] which were then thought to provide a favourable solution to companies seeking to transfer data outside the EU or EEA. These clauses however proved to have short comings and the take up rate was slower than expected. For example, both parties in the transfer process were deemed to be jointly and severally liable to the individual and the data exporter was required in cases of sensitive personal data to provide a warranty to the individual concerned. In 2004, the Commission approved a new set of contractual

---

[62] See section 2.4

[63] See APEC Information Privacy Framework (Review, Impact and Progress) , APEC Symposium on Information Privacy Protection in E-Government and E-Commerce, Viet Nam 2006 available at http://www.apec.org/content/apec/documents_reports/electronic_commerce_steering_group/2005.html#SEMHK

clauses[65]. The alternative clauses provide a more equitable split of liability as parties are now only liable for their own breaches and there is overall more flexibility for the organizations concerned[66]. However, the fact remains that a contract still needs to be in place between all exporters and importers and this may not be the most suitable arrangement for multinational organizations who need to transfer data internally. Thus, the Commission's attention has recently been focused on the use of binding corporate rules (BCRs) to govern internal transfers within multinational organizations.

This development has not escaped APEC's attention and in the recent Symposium in Viet Nam in February 2006, discussion on the implementation of the APEC Privacy Framework revolved on the use of BCRs and the next steps that businesses can take to pioneer this development[67] rather than calling for work on standard contractual clauses.

Therefore while APEC Privacy Framework does not explicitly address the issue of cross border data transfer, it does call for cooperative development of cross border privacy rules in Part B. In this way, the APEC Privacy Framework is still able to address the problems that corporations face with regards to data transfer and benefit from the lessons that the EU has learnt through trial and error.

As for the weaknesses of the APEC Privacy Framework, this can be grouped into 2 categories. The first relates to the nature of the APEC Privacy Framework as a legally binding instrument. The second relates to the principles contained in the Framework.

With regards to the first weakness, the criticisms relating to the lack of a central enforcement body and the potential for variances in implementation are valid and are recognized by APEC itself. Section 39 of the Framework provides that Member

---

[64] Commission Decision of 15 June 2001 OJ L 181/19
[65] Commission Decision of 27 December 2004, OJ L385/74
[66] For a more detailed treatment, see *Data transfer contracts- a new option for cross border transfers* , Alexander Brown, Lucy Pownall, Privacy Laws & Business International Newsletter, January/Feb 2005, Issue 76

Economies should make known the status of their domestic implementation through periodic updates in their Individual Action Plan reports. Furthermore, it encourages Member Economies to participate in sharing information, surveys and research as well as cross border cooperation in investigation and enforcement[68]. During the recent Symposium in Viet Nam in February 2006, strategies such as establishing a single, government backed authority or a Non-Governmental Organization such as an 'APEC Privacy Commission' to engage, encourage, assist and enforce the APEC Privacy Framework when more than one Member Economy was involved were also discussed[69]. This is heartening as it suggests that future improvements are at least under consideration and that APEC is aware of its limitations as a voluntary grouping.

With regards to the second category of weakness, this is perhaps the more troubling set. Professor Graham Greenleaf who has written extensively on the drafting of the APEC Privacy Framework[70] has noted the weakness in basing the APEC Privacy Framework on the OECD Guidelines which are more than 20 years old. For example, the OECD Guidelines do not include any principles dealing explicitly with identifiers, automated processing or deletion of data.

Furthermore, Professor Greenleaf is of the view that the APEC Privacy Framework is weaker than the existing OECD Guidelines because of the missing OECD Principles of a) Purpose Specification, b) Data Export Limitation and c) Openness. With regards to a) Purpose Specification, arguably, this is implied by the Notice Principle read together with the Choice Principle and Uses of Personal Information Principle. As shown in Annex A, the core value embodied by the Purpose Specification Principle is that of

---

[67] Supra footnote 63
[68] See paragraphs 40-45 of the APEC Privacy Framework
[69] Supra footnote 63
[70] See The APEC privacy initiative: "OECD Lite" for the Asia Pacific, available at www.bakercyberlawcentre.org, in relation to the 8th draft of the APEC Privacy Framework and supra footnote 7 in relation to the 9th draft of the APEC Privacy Framework.

ensuring that Personal information should be collected for specified, lawful or legitimate purpose and not be processed incompatibly from those purposes[71].

Similarly, b) the Data Export Limitation Principle was replaced by a conscious choice of the Principle of Accountability which as described above is an approach more in line with modern business practices and the stated purpose of the APEC Privacy Framework.

However, it is disappointing that c) the Openness Principle was dropped as in practice without this right, it is difficult for an individual to ascertain the existence and the nature of the data held by organizations about him or her. A related development during the Symposium at Viet Nam 2006, was that while a template for the Individual Action Plans ("IAP") was endorsed by the E-Commerce Steering Group and a timeline of November 2006 was set for the filing of these reports, it was clarified that the IAP did not apply to e-government related matters although a government can choose to report on these matters if it chooses to[72]. This is a strange development as the APEC Privacy Framework is not limited to the private sector and even states expressly that 'The APEC Privacy Framework applies to persons or organizations in the public and private sectors who control the collection, holding, processing, use, transfer or disclosure of personal information.'[73] This action only serves to increase concerns that a culture of governmental secrecy is being propagated.

Additionally, Professor Greenleaf is of the view that the elevation of "choice" as separate principle in the APEC Privacy Framework, in contrast with the existing international instruments, facilitates the commodification of privacy. Professor Greenleaf cautions against the interpretation that individual consent can override the other Principles.

---

[71] See Annex A

[72] See *APEC's privacy framework on show in Vietnam: how much progress?* Graham Greenleaf, Privacy Laws & Business International Newsletter, May 2006

While the writer agrees with Professor Greenleaf's conclusion that the APEC Privacy Framework is probably inadequate as the definitive set of privacy principles for Asia Pacific countries, the APEC Privacy Framework is perhaps not intended to be such a vehicle. The foreword to the Framework puts its objectively plainly, it is to "enable regional data transfers [that] will benefit consumers, businesses and governments". Paragraph 4 of the Preamble goes on to state that the Framework is 'an important tool in encouraging the development of appropriate information privacy protections and ensuring the free flow of information in the Asia Pacific region.'

Seen from this context, the Choice Principle read together with the Notice Principle make perfect sense to the consumer and the business or government involved. It is formulated specifically to address the problems that might arise from economic aspects of global trade. Therefore, the application of Framework is specifically left to each Member Economy and section 12 endorses a flexible implementation of the same. Accordingly, it appears that the APEC Privacy Framework vis-à-vis the Directive is a completely different creature from its underlying rationales, its objectives and its emphasis on aspects of informational privacy principles.

4 At the crossroads- The Singaporean experience

What does the APEC Privacy Framework mean for its Member Economies? How are the Member Economies going to implement its principles into their domestic legislation? It is perhaps a little to early to say as the first IAPs have yet to be filed.

---

[73] See Part II of the APEC Privacy Framework, commentary on paragraph 10.

Nevertheless, it would be helpful to examine the initial responses its Member Economies have towards the APEC Privacy Framework in order to predict what kind of long term effect it is likely to have.

I have chosen to examine Singapore's response. Singapore is *tabula rasa* in the sense that it does not have a general and comprehensive data protection law in force. The right of privacy is not explicitly recognised in its Constitution. Singapore is also not a signatory to international conventions recognizing the right of privacy such as the International Convention on Civil and Political Rights, neither is it bound by the European Convention of Human Rights.

At the same time, Singapore is keen to position itself as an international e-commerce hub. As stated by the government ministry in charge (Infocomm Development Authority 'IDA') on its website "One of IDA's key roles is to develop the Singapore infocommunications industry into a key engine of growth for the economy"[74]. For instance, IDA released its 5th Infocomm Technology Roadmap on 8 March 2005 which highlighted the potential of sensor technology, biocomputing, nanotechnology and other emerging technologies. The use of sentient technologies is also envisaged to enhance the quality of life such as smart systems to sense and remind elderly patients at home to take their medication and tracking systems, biosensors and wearables that will create more exciting lifestyles in smart homes and entertainment applications for the masses.[75] The latest programme unveiled by the IDA is called Intelligent Nation 2015 (iN2015)[76]. It is an ambitious plan to transform key economic sectors, government and society through the use of infocommunications.

---

[74] See http://www.ida.gov.sg/idaweb/pnr/infopage.jsp?infopageid=I781&versionid=2 for a list of existing initiatives in place to develop the infocommunications industry in Singapore

[75] See media release dated 8 March 2005 http://www.ida.gov.sg/idaweb/media/infopage.jsp?infopagecategory=technology.mr:media&versionid=6&infopageid=I3337

[76] See http://www.in2015.sg/about.html for overview and detailed reports

Singapore was ranked 1st in 2004/2005 and 2nd in 2005/2006 by the World Economic Forum in its Global Information Technology Report. This report measures the ability of individuals and government to tap into the potential of infocommunications technology, as well as the government usage of infocommunications technology[77].

Thus, in the writer's view, Singapore is an ideal case study to examine how economic concerns instead of human rights concerns will shape the legislative response to data protection issues.

4.1 Introduction to Singapore's legal system

Singapore's legal system is based on the English common law.

The current position in Singapore is that under common law, an enforceable right to privacy does not exist.

One writer[78] summarizes the position succinctly as follows: Assuming that privacy is accepted to encompass four related groups of torts that deal with a) unreasonable intrusion on the seclusion of another, b) appropriation of another's name or likeliness, c) unreasonable publicity given to another's private life and d) publicity that unreasonably places the other in a false light before the public, there are a few causes of action that may arise in respect of each category.

For instance, in respect of the intrusion into seclusion or solitude, trespass to the person (assault, battery and false imprisonment), trespass to land, nuisance, harassment and even the intentional infliction of nervous shock may be relevant. For the second category, the tort of passing off and registered trade mark infringement may be used. For the third category, an action in equity to protect confidential information can be

[77] The reports are available at www.weforum.org/gitr

used to protect against unwanted publicity for private facts. For the final category, defamation and malicious or injurious falsehood are the main actions that come into play.

These however suffer from limitations, as obviously certain conditions have to be met before a cause of action can arise. In particular for actions arising from the first category, under English law, the law of private nuisance is traditionally a tort against the enjoyment of land. The House of Lords reaffirmed in *Hunter v Canary Wharf Ltd*[79] that a person must have interest in the land to have standing to sue. The tort of trespass is likewise based on one's property right.

The tort of harassment however does not suffer from such limitations. For instance, in *Malcomson Nicholas Hugh Betram v Naresh Kumar Mehta*[80] the tort of harassment was accepted by the Singapore Court as a valid cause of action to deal with interfering acts that did not arise from the Plaintiffs' interest in land[81].

In this case, the Defendant was employed as an Assistance Vice President of the Plaintiffs. The first Plaintiff was the Chief Executive Officer. The employment did not go well and the Defendant left the company. Thereafter, for about a period of 1 year, the Defendant made and sent numerous phone calls and emails to the Plaintiffs. The Defendant managed to obtain the 1st Plaintiff's home address and sent him a congratulatory card close to the anniversary of the death of the 1st Plaintiff's son.

In his judgment for the Plaintiffs, then Judicial Commissioner, Lee Seiu Kin observed[82]

---

[78] *Milky Way and Andromeda: Privacy, Confidentiality and Freedom of Expression* [2006] 18 SacLJ 1 at pp 8-13 George Wei

[79] [1997] 2 All ER 426

[80] [2001] 3 SLR 454

[81] It is to be noted that the *Malcomson* decision was a default judgment as the Defendant had failed to file his Defence in time. The question of whether the tort of harassment exists under common law has yet to reach the Singapore Court of Appeal for consideration. For a detailed discussion of *Malcomson*, see Tan Keng Feng "Harassment and Intentional Tort of Negligence" [2002] Sing JLS 642

[82] Supra 80, see paragraph 55

> "life can be unbearable for the person who finds himself the object of attention of one who is determined to make use of these modern devices to harass. That person's mobile phone can be ringing away at all times and in all places. He may get a flood of SMS messages, which can now be conveniently sent out by computer via email… I do not believe that it is not possible for the common law to respond to this need. In Singapore we live in one of the most densely populated countries in the world."

However, while the tort of harassment goes some way to protecting privacy in the sense of the right to be left alone, it is obviously not satisfactory as a data protection regime. It does not address issues such as providing individuals with control over the use and disclosure of their personal information or other core principles such as the fair collection and processing of data. See section 2.1.3 above where the principles are discussed. This comment applies equally to the other categories of causes of action[83].

Turning to legislation in force in Singapore. As stated earlier, there is no general privacy or data protection act.

There are however many statutes that touch upon the processing of personal data in specific contexts. For instance, information relating to governmental matters is expressly protected from unauthorised disclosure under the Official Secrets Act (Cap 213). Sector specific statutes that deal with secrecy and disclosure provisions apply to the private sector as well, for instance the Banking Act (Cap 19) and the Legal Professions Act (Cap 161). All in all, about 161 separate statutes have provisions that touch upon secrecy and disclosure provisions[84].

---

[83] As the focus of this paper is on data protection regimes, the writer will not venture into a detailed discussion of the current state of common law actions in Singapore jurisprudence that impact on the right of privacy. For an enlightening discussion on these issues, see supra footnote 72.

[84] See report by the NIAC subcommittee on the Model Code, available at http://www.agc.gov.sg/publications/docs/Model_Data_Protection_Code_Feb_2002.pdf

However, 'data protection' provisions in Singapore have traditionally taken the approach of regulating only the common forms of 'processing' such as collection and disclosure. Issues such as rights to access and correction, accuracy, retention and data security are not addressed by most of the existing laws.

It was only with the emergence of e-commerce that businesses and governmental bodies in Singapore became aware of the issues of data protection. The first piece of relevant regulation albeit a voluntary code was issued in 1998 by the National Internet Advisory Committee (NIAC). This was the "E-Commerce Code for the Protection of Personal information and Communications of Consumers of Internet Commerce". The Code was adopted as part of a voluntary accreditation scheme called CaseTrust for consumer businesses.

It was around this period that the Directive and its influence on international legislation became apparent. The NIAC thus started work on a new code that would specifically address the requirements of the Directive. The NIAC released a new code entitled the Model Data Protection Code for the Private Sector in 2002[85]. The Model Code is modelled after the Canadian Standards Association's Model Code for the Protection of Personal Information (CSA Code) which in turn in based on the OECD Guidelines[86]. The Model Code, which is organised around 10 data protection principles establishes the minimum standards for how personal data may be managed and processed by private sector organisations. The Code achieves this by defining and imposing limits and restrictions on the processing of such data.

The Model Code is currently in use in a voluntary data protection scheme co-ordinated by the National Trust Council which is a cooperation between the government and the industry. The National Trust Council evaluates and nominates companies to act as

[85] Available online at TrustSg, http://www.trustsg.com/radiantrust/tsg/rel1_0/html/downloads/Data_Protection_Code_v1.3.pdf

Authorised Code Owners. These Authorised Code Owners then evaluate other companies and award them with the 'Trustsg' trust mark if they fulfil the criteria set out in the Model Code.

The NIAC report[87] further stressed the need for a harmonised, comprehensive data protection regime in Singapore as proliferation of data protection regimes and practices is confusing to consumers and makes monitoring and auditing by relevant authorities difficult. On the other hand, harmonised regimes translate into lower operational costs for global businesses.

The Committee also examined the different models of enforcement and compliance options although this was strictly outside the ambit of the Committee's study[88] and concluded that a comprehensive and co-regulatory data protection model was the most compelling model for Singapore to adopt. It is interesting to note is that the NIAC in their report had specifically stated that the Model Code is meant only as an interim measure.

As it stands today, it is unlikely that Singapore will pass the adequacy requirement imposed by the Directive due to the fragmented nature of its legislation, common law and voluntary codes of conduct and the lack of enforcement options[89].

4.2 Current and future developments

There is an increasing concern voiced by the public about the use and processing of their personal data. This has been acknowledged by the government.

---

[86] For criticisms of the Model Code, see *Singapore Takes the softest privacy options*, Privacy Law & Policy Reporter, Vol 8, No 9 March 2002, Graham Greenleaf
[87] Supra 84, Paragraph 5.15 of the report onwards
[88] Ibid, See section 6 of the report
[89] For a detailed analysis, see *European Data Protection Directive: Adequacy of Data Protection in Singapore*, [2004] Sing JLS 511, Vili Lehdonvirta

At the Parliament sitting on 14 February 2006, the Minister for Information, Communications and the Arts Lee Boon Yang was asked whether privacy laws would be introduced in Singapore[90]. The Minister replied stating that "the Government recognises the increasing importance and impact of data protection in Singapore and the need to protect a person's personal data and prevent the possibility of misuse of personal information or identity theft" and that the Government recognises that "an effective data protection regime will be an important pillar to develop Singapore 's position as a trusted IT- hub. It will also be a critical factor in building trust between consumers and businesses for the adoption of new technologies and services (such as electronic transactions, biometrics and RFID)."

The Minister revealed that the Government had started examining the issue in November 2004 and had formed an inter-ministry panel in October 2005. (This was around the same time that the first part of the APEC Privacy Framework was released.) 16 governmental agencies are involved and are due to release their recommendations by the middle of 2006.

At another Parliamentary debate on 3 March 2006[91], the Minster in response to Professor Chin Tet Yung's question about data protection made the following statement:

> "I agreed that we must take a comprehensive approach. On 13 Feb 06, I informed the House that the Government is already reviewing Singapore's data protection regime and assessing the suitability of various data protection models.

---

[90] See press release at http://www.mica.gov.sg/Parliament/Sitting%2014-02-06.htm and news report "Personal Data: Panel Looking at Protection", Straits Times 15 Feb 2006, Goh Chin Lian
[91] See press release at http://www.mica.gov.sg/pressroom/press_060303.htm

> I would like to reassure the House that the government recognises the importance and impact of data protection on Singaporeans. We cannot shut out new technologies including those that can be abused. We have to strike a right balance between facilitating the adoption of new technologies and protecting personal data."

A follow up inquiry with the Ministry of Information, Communications and the Arts (MICA)[92] led to an updated statement as follows: "MICA and IDA are currently reviewing the issue of data protection. MICA and IDA is working with the relevant agencies in the private and public sectors, to assess the suitability and effectiveness of various data protection regulatory models for Singapore, and will be announcing the updates sometime this year."

The recommendations and press release are expected to be released before the end of the year[93].

More recently, it was reported that Singapore is joining Australia, Canada and USA in a study group on information sharing and cross border cooperation with regards to the APEC Privacy Framework[94].

These are all encouraging signs that there will be continuing work on the issue of data protection in Singapore. From the statements issued by the Minister and the NIAC, it is highly possible that a comprehensive data protection model will recommended in the upcoming report.

---

[92] Email dated 19 July 2006 from the Ministry's Corporate Communications Department to the writer
[93] Email dated 15 August 2006 from the Ministry's Corporate Communications Department to the writer
[94] *News*, page 5 Privacy Laws & Business International Newsletter, May 2006, Issue 82

5 The future- A movement towards global standards?

5.1 A growing acceptance of what amounts to Fair Information Practices

While at first glance there appears to be deficiencies in the APEC Privacy Framework, its value should not be overlooked. The APEC Privacy Framework represents a consensus between countries who come from different legal systems, different values and are at different stages of enacting their privacy legislation. Furthermore, it involves countries, for instance China and the South East Asian nations, who were not previously party to any international agreement regarding data protection and privacy but who are emerging players in the world economy. It is submitted that the immediate value of the APEC Privacy Framework is more akin to the CoE Convention than the Directive in that it forms the basis for the APEC countries to acknowledge and implement basic principles of data protection.

The APEC Privacy Framework further provides impetus for governments to look into the larger picture and review the existing state of their privacy legislation. While the APEC Privacy Framework itself is primarily focused on e-commerce, it would be anomalous to have a set of principles applicable only for this one area of activity. While the APEC Privacy Framework is also non prescriptive with regards to cross border data flows, again domestic implementation will invariably highlight this issue and it would be strange to ignore this particular aspect. For instance as discussed in section 4.2, Singapore is currently in the process of reviewing its current legislation and deciding whether or not it needs to implement comprehensive data protection legislation across the board. Singapore is also participating in a study relating to cross border cooperation.

5.2 An emerging dialogue

While the EU model is widely accepted as providing a comprehensive and high standard of data protection, even after 10 years, harmonization within the EU is not yet complete[95]. It is not realistic for the EU to have to certify the adequacy of every non EU countries' data protection laws especially with globalisation of trade and the emergence of e-commerce. As one writer comments, the EU is caught "between a rock and a hard place: if properly implemented, the regime is likely to collapse from the weight of its cumbersome, bureaucratic procedures. Alternatively, it could well collapse because of large scale avoidance of its proper implementation due precisely to fears of such procedures."[96]

That being the case, would an international standard be the best way forward? There have been previous discussions whether the data protection question should be taken up by the world's standards setting and certification bodies. The rationale behind this proposal is that a privacy protection could be regarded as an element of 'quality management', similar to that of the ISO 9000 series of quality management.

5.3 A race to the top or the bottom or…?

One writer[97] writes that an international standard would give businesses outside Europe a more reliable and consistent method by which to demonstrate their conformity to international data protection standards. It would also be easier to implement Article 25 of the Directive instead of having to scrutinize each country's state of laws and contracts. In the late 1990s, the International Standards Organization (ISO) considered the idea of developing an international standard for the protection of personal information. However, due to the inability to formulate what form the standard should

---

[95] *'2005 marks 10th Anniversary of the EU Data Protection Directive'* Privacy Laws & Business International Newsletter, December 2005, Issue 80
[96] See Bygrave (2004)
[97] See Bennett, Colin (2002)

take and what its relationship with the Directive's position on cross border data transfer would be, ISO abandoned work on the standard in 1998. It concluded that it was premature at that time to develop an international data protection standard[98].

Alternatively, there have been calls by privacy commissioners for the United Nations to prepare a convention on data protection. This was made following the 27th International Conference of Data Protection and Privacy Commissioners held in Montreux, Switzerland on 14-16 September 2005[99]. In the Declaration, 5 existing international instruments were recognized with regards to the principles of data protection, the APEC Privacy Framework was one of them.

APEC's recognition of a set of principles based on OECD Guidelines is proof that there can be a common international consensus on what it means to treat personal information in a privacy-friendly manner. There is also an increasing awareness globally about the need to protect privacy and personal data in the interconnected and technologically advanced world that we live in.

Perhaps the time is ripe for a re-evaluation of the possibility of a global standard, be it by way of an international standard or a truly international convention, for data protection. While the process is not going to be easy or short, the APEC Privacy Framework is one step towards that final destination.

---

[98] For further discussion, see *"An International Standard for Privacy Protection: Objections to the Objections"*, Colin J. Bennett.
http://web.uvic.ca/polisci/bennett/pdf/ilpf.pdf

[99] See page 3, sub-paragraph (a) of the Montreux Declaration available at www.privacydataprotection.co.uk/documents/**montreux_declaration**.pdf See also *Commissions call for an international Privacy convention*, Privacy Law Bulletin, Vol 2 No 6, Saira Ahmed & Prashanti Ravindra

6 References

List of Judgements/Decisions

Durant v FSA (2003) EWCA Civ 1746

Hunter v Canary Wharf Ltd [1997] 2 All ER 426

Malcomson Nicholas Hugh Betram v Naresh Kumar Mehta [2001] 3 SLR 454

Treaties/Statutes

CoE Convention	1981 Convention for the Protection of Individuals with regard to the Automatic processing of Personal Data
OECD Guidelines	1980 Guidelines Governing the Protection of Privacy and Transborder Flows of Personal Data
UN	1990 Guidelines Concerning Computerized Personal Data Files
Directive 95/46/EC	Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data
APEC Privacy Framework	Asia-Pacific Economic Cooperation Privacy Framework 2004
The Montreux Declaration	The protection of personal data and privacy in a globalised world: a universal right respecting diversities

Secondary Literature

Bygrave, L.A (2002)	*Data Protection Law: Approaching its Rationale, Logic and Limits*, Aspen Publishers Inc
Bygrave, L.A (2004)	*Privacy Protection in a Global Context- A Comparative Overview*, Scandinavian Studies in law, 2004, Vol 47 p 319
Bennett, Colin (2002)	*Information Policy and Information Privacy- International Areas of Governance*, available at

http://web.uvic.ca/polisci/Bennett

"*An International Standard for Privacy Protection: Objections to the Objections"*, available at http://web.uvic.ca/polisci/bennett/pdf/ilpf.pdf

Bennett & Raab (2003) — *The Governance of Privacy: Policy Instruments in Global Perspective*, Ashgate

Bainbridge (1996) — *The EC Data Protection Directive*, Butterworths, London

Brown, Alexander and Pownall, Lucy — *Data transfer contracts- A new option for cross border transfers*, PL&B International, Jan/Feb 2005 Issue 76

European Commission — Seventh report on the situation regarding the protection of individuals with regard to the processing of personal data and privacy in the European Union and in third countries covering the years 2002 and 2003

First report on the implementation of the Data Protection Directive 95/46/EC

Special Eurobarometer on Data Protection

Working Party — Working Document: Transfers of Personal data to 3rd countries: Applying Articles 25 and 26 of the EU Data Protection Directive
("WP 12")

Graham Greenleaf — *Singapore Takes the softest privacy options*, Privacy Law & Policy Reporter, Vol 8, No 9 March 2002

The APEC Privacy Initiative: "OECD Lite" for the Asia Pacific (v8) available at www.bakercyberlawcentre.org

Criticisms of the APEC Privacy Principles (v9) and recommendations for improvement, available at www.bakercyberlawcentre.org
.
APEC Privacy Framework: A new low standard PL&B International, Jan/Feb 2005, Issue 76

APEC Privacy Framework completed: No threat to privacy standards. PL&B International Sep/Oct 2005, Issue 79

APEC's privacy framework on show in Vietnam: how much progress? PL&B International, May 2006

Jay & Hamilton (2003)	*Data Protection-Law and Practice*, Sweet & Maxwell
Lehdonvirta,Vili	*European Data Protection Directive: Adequacy of Data Protection in Singapore*, [2004] Sing JLS 511
Linkomies, Laura	*Slow Progress on the EU Privacy Programme*, PL& B International Oct/Nov 2004
Saira Ahmed & Prashanti Ravindra	'*Commissioners call for an international privacy convention*' Privacy law Bulletin, Vol 2 No 6 November 2005
Tan Keng Feng	*Harassment and Intentional Tort of Negligence* [2002] Sing JLS 642
Usha Jagessar, Vicky Sedgwick (2005)	*When is personal data not 'personal data'- The impact of Durant v FSA*, Computer Law & Security Report (2005) 21 p501-511
Wei, George	*Milky Way and Andromeda: Privacy, Confidentiality and Freedom of Expression* [2006] 18 SacLJ 1

7 Annex