UiO : Faculty of Law
University of Oslo

# The adequacy requirement: selectively flexible or unjustifiable discrimination?

A critical analysis from an Australian perspective

Candidate number: 8012

Submission deadline: 31 May 2013

Supervisor: Dr Lee Bygrave

Number of words: 17,942 (max: 18,000)

Semester: Spring 2013

Date of submission: 31 May 2013

## Abstract

Adequacy of data protection and privacy is an essential feature of Article 25 of the EU Data Protection Directive 95\46\EC. Despite this, the adequacy criterion has been applied inconsistently to the information privacy protection instruments of third countries of analogous jurisdiction. This is because the adequacy criterion is inconclusive and, therefore, open to inconsistent application. This inconclusiveness also enables the A29WP and the European Commission ('the Commission') to selectively alter the adequacy criterion to consider its trade relationships with third countries when determining adequacy. This occurred when the Commission found adequacy in the US *Safe Harbour Agreement (*US *SHA),* and during the A29WP's assessment of New Zealand *Privacy Act 1993* (the *NZ Act*).

On the other hand, the *Australian Privacy Act 1988 (the Australian Act)* was found not to offer an 'adequate' level of information privacy protection for the purpose of Article 25(1) of the *Directive*. This determination was made on a strict application of the adequacy criterion and without any regard for the trade relationship between the EU and Australia.

The adequacy of the *Australian Act* is again relevant as it undergoes substantive reform, although predicting whether the Commission and the A29WP will find adequacy is wrought with unpredictability. Australia may instead consider looking to the WTO for an assessment of the EU's strict assessment of the *Australian Act* in comparison to more lenient assessments of the US *SHA* and the *NZ Act* in light of the requirement for non-discrimination at Article XIV of the *General Agreement on Trade in Services 1994*

## Acronyms

ALRC – Australian Law Reform Commission

APEC – Asia Pacific Economic Cooperation

A29WP – Article 29 Data Protection Working Party on the Protection of Individuals with Regard to the Processing of Personal Data

ECJ – European Court of Justice

EEA – European Economic Area comprising the countries of the EU (and Croatia as of July 2013), plus Iceland, Liechtenstein and Norway.

EU – European Union

The *Gats* – General Agreement on Trade in Services 1994

OECD – Organisation for Economic Cooperation and Development

US – The United States of America

WTO – World Trade Organisation

## Table of Contents

## Acknowledgements

The author is grateful to the Norwegian Research Centre of Computers and Law, where this thesis was completed as part of an International Masters of Information and Communication Technology Law. The author also wishes to thank Dr Lee Bygrave for his valuable comments and suggestions on previous drafts.

# 1 Introduction

## 1.1 Overview

Adequacy of data protection and information privacy is an essential feature of Article 25 of the EU Data Protection Directive (the *Directive*)[1]. It mandates a restriction on the transfer of personal information to third countries [2] such as Australia, which the European Commission (the Commission) and the A29WP (in its application of its adequacy criterion) have deemed do not ensure an 'adequate level of protection'. The *Australian Privacy Act 1988*[3] *(Australian Act)* was denied an adequacy rating for the purpose of Article 25(1) of the *Directive* by the Commission in 2001.

Despite the emphasis on adequacy in the *Directive*, the A29WP and the Commission have applied their adequacy criterion inconsistently to the information privacy protection instruments of countries of analogous[4] jurisdiction to Australia, such as the US *Safe Harbour Agreement* (*SHA*)[5], and the *New Zealand Privacy Act* 1993 (the *NZ Act*).[6] This is because the inconclusiveness of the adequacy criterion leaves the *Directive* open to inconsistent application. This has resulted in the Commission and the A29WP selectively altering the adequacy criterion to consider the EU's trade relationship with third countries as a determinative of adequacy.

Article 25 (1) of the *Directive* reflects the EU approach to protecting privacy, and enables the EU to pass judgment on the information privacy protection systems of the third countries it assesses. However, the European approach is not always consistent with the approach

[1] 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* [1995] OJ L281/31

[2] Third countries is the term employed by the *Directive* to distinguish countries beyond EEA borders

[3] Act No.119 of the Australian Parliament [1988] (as amended)

[4] For an explanation of 'analogous': ch4.1 of this thesis

[5] Commission decision 2000/520/EC *on the adequacy of protection provided by the 'Safe Harbor' privacy principles and related frequently asked questions issued by the US Department of Commerce* (1999) [WP 27]

[6] Act No.28 of the New Zealand Parliamentary Council Office [1993] (as amended)

taken by third countries that preserve varying approaches to privacy protection in their relevant legislation. This further complicates the adequacy assessment process.

However, the mandated restriction on the transborder transfer of EU citizens' personal data at Article 25(1) of the *Directive* is imposed unless one of the derogations prescribed by Article 26 of the *Directive* applies; for example, the employment of contractual measures (*contract derogation*) as a means of providing further safeguards for data transfers. Thus, *Australian* organisations preserve their trade relations with EEA-based organisations on the basis of the *contract derogation* in light of *Australian Act* being decided as non-adequate. This decision of non-adequacy resulted from a stricter application of the adequacy criterion to the *Australian Act*, than more lenient and trade-based assessments of the US *SHA* and the *NZ Act*.

The US *SHA* and the *NZ Act* have both received adequacy ratings; however, the reasons for the granting of adequacy in these cases were inconsistent with the reasons given for the denial of adequacy in relation to the *Australian Act*. Those findings of adequacy reflect an alteration to the adequacy criterion to take into account their trade relationship with the EU.

Furthermore, a comparative analysis of the A29WP and the Commission's treatment of the *Australian Act*, the US *SHA*, and the *NZ Act* raise questions about the possibility of discriminatory treatment of the *Australian Act* in light of Article XIV of the WTO *General Agreement on Trade in Services 2004* (the *Gats*).

## 1.2 Research questions

The adequacy requirement has achieved an elevated status on the basis that the EU imposes that requirement on the privacy protection instruments of third countries, as it did when assessing the adequacy of the *Australian Act*, the US *SHA*, and the *NZ Act*. However, the strict application of the adequacy criterion to the *Australian Act* when examined in light of more trade-motivated approvals of the US *SHA* and the *NZ Act* raise a number of questions requiring address. These include:

- Is the inconclusive adequacy criterion susceptible to being applied inconsistently?

- Was the adequacy criterion applied more strictly to the *Australian Act* than the systems of the US *SHA* and *NZ Act?*

- Do the Commission and the A29WP selectively alter the adequacy criterion to include trade considerations as an overriding determinative of adequacy in their assessments of information privacy protection instruments of certain third countries (the US and New Zealand) but not when assessing relevant legislation of other third countries (Australia)?

- Does the above constitute arbitrary or unjustifiable discrimination under Article XIV of the *Gats*?

### 1.3 Methodological issues

The primary focus of this thesis is the adequacy requirement at Article 25 of the *Directive.*

This thesis applies traditional legal dogmatics to provide commentary on the adequacy requirement in the context of transborder data transfers: its interpretation in the formulation of the A29WP's adequacy criterion, and the subsequent application of the adequacy criterion to the relevant legislation of analogous third countries namely, Australia, the US and New Zealand.

This thesis includes a discussion of the differing European and Australian legal approaches to information privacy protection as an example of why applying the adequacy requirement to third countries is wrought with difficulty. This comparison was chosen because a strict application of the adequacy criterion to the *Australian Act* resulted in a finding of non-adequacy, and because the *Australian Act* is currently undergoing reform. On the other hand, a more lenient application of the altered adequacy criterion to the US *SHA* and the *NZ Act* produced findings of adequacy.

## 1.4 Thesis structure

This thesis has five chapters including the introductory part.

The second chapter elaborates on the European approach to information privacy protection as reflected in the *Directive,* and through the adequacy assessment process undertaken by the A29WP and the Commission.

The third chapter analyses the A29WP's application of the adequacy criterion to the *Australian Act*. That chapter also focuses on aspects of the *Australian Act* that the A29WP deemed to be barriers to a finding of adequacy, but that also highlight instances where the Commission and the A29WP have misinterpreted the *Australian Act*. These aspects also reflect differing continental- approaches to the act of legislating for information privacy protection.

The fourth chapter provides a comparative analysis between the adequacy findings for the US *SHA* and *NZ Act* and the non-adequate *Australian Act*. This chapter deals with how the A29WP and the Commission selectively alter the adequacy criterion to include trade considerations where the US *SHA* and *NZ Act* were concerned.

Chapter five addresses the possible implications arising from the inconsistent application of the adequacy criterion to the US *SHA*, the *NZ* Act, and the *Australian Act* in light of the requirement of non-discrimination under Article XIV of the *Gats*.

The author's conclusions are then provided.

# 2 Protecting Information Privacy in Transborder Data Transfers

## 2.1 Definitional issues

The clarification of terms such as 'privacy', 'data protection', 'transborder transfers', and 'adequate' is crucial to understanding the application of relevant laws to transborder data transfers among individuals, private entities and government institutions. This is particularly important in contemporary society where such transfers are a ubiquitous feature of modern day electronic commerce, and thus require legislative protection.

*Privacy*

'Privacy' has been referred to as an 'elusive concept that is difficult to define in any satisfactory manner'[7]. Heisenberg[8] comments that, internationally, there are different constitutional orders, legal systems, and interpretations of privacy. Thus, this variance leads to different interpretations of the right to privacy. Indeed, the level of right afforded to it by the EU, in contrast to that afforded by the third countries upon which the EU purports to impose its adequacy requirement, forms the basis of some of the tension surrounding the application of Article 25 of the *Directive*.

*Data Protection*

The term 'data protection' (from the German 'Datenschutz'), on the other hand, is generally accepted as a standard formulation of the right of individuals to protect information about themselves from being widely disseminated or stored indefinitely. Weber[9] defines data protection as covering specific aspects of privacy that give rights to individuals in respect to how data identifying them or pertaining to them are processed, and that this processing is

[7] ALRC (1983) p.19
[8] (2005) p.13
[9] (2012) p.30

subjected to a defined set of safeguards. Throughout this thesis, the terms 'personal information privacy', 'privacy protection', 'data protection' and 'data privacy' are used interchangeably.

*Transborder Data Transfers*

The situation of protecting personal information privacy in transborder transfers is further complicated by the absence of a universally accepted legal definition of 'transborder transfers', which is also confused with 'cross-border' or 'transborder data flows'.

The *Directive* does not define a 'cross-border transfer' of personal data. However, some light was shed on the concept when the ECJ considered the concept in the case of *Bodil Lindqvist* (the *Lindqvist* decision)[10], establishing that a 'transfer' only exists when there is a 'direct transfer' between the person who uploaded the data and the person in a third country.

In an attempt to define transborder data transfers, the ALRC[11] stated that such transfers are accepted as referring to the export of personal information across jurisdictional boundaries. Despite the non-existence of a universally adopted definition of cross-border or transborder data transfers, and the ambiguity of the 'transfer' concept[12], it is generally accepted that individual persons who process data in a non-business capacity are exempt from the respective frameworks.[13]

*Adequate*

As we will see below, 'adequate' as prescribed by Article 25(1) of the *Directive* is also not exempt from definitional ambiguity. This results in practical difficulties for the EU when it purports to impose the adequacy requirement on the third countries it assesses.

[10] Case C-101/01 [2003] ECR I-12971
[11] The *ALRC* is an Australian federal agency that reviews Australia's laws for example, it reviewed Australia's information privacy legislation in 2008
[12] For a summary of the ambiguity of the transfer concept: Esayas (2012) p, 664-665; Kuner (2007) p.82
[13] For example: *Australian Act,* Section 7B(1); *Directive*, Article 3(2) as interpreted by the ECJ in the *Lindqvist* decision

## 2.2 The European approach

The *Directive*, which applies to member states of the EEA, seeks to uphold individuals' right to privacy in relation to the collection, use and dissemination of personal data[14]. The right to privacy is upheld to the extent that it reflects the view that the right to information privacy is on par with the respect for privacy, generally, as a fundamental human right[15]. In the *Rechnungshof Case*[16], for example, the ECJ interpreted the *Directive* to apply to the processing of personal data, and to ousting the application of rules of national laws which are contrary to the provisions of the *Directive*. Thus, while the *Directive* is believed to act as a general framework[17], it is far-reaching and reflects the emphasis placed on the right to privacy under the European approach. This approach to regulation taken by the EU is described as the 'Franco-German bureaucratic approach'[18], and is founded in the rights-based deontological theory.[19] Thus, the *Directive*, particularly Article 25(1)[20], reflects a European tendency for data protection rules that entail negative limits on data processing activities[21] by way of laws that provide the possibility for non-compliance to be sanctioned, and for individuals to be given a right to redress.[22]

[14] 'Personal Data' as defined by the *Directive*, Article 2 (a): '[…] Any information relating to an identified or identifiable natural person….an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number, or to one or more factor specific to his physical, physiological, mental, economic, cultural or social identity[…]'

[15] The *Treaty on the Functioning of the European Union*, Article 16 was introduced to replace the now non-existent *EU Charter of Fundamental Rights 2000* as a new constitutional basis for personal data protection in the EU. This protection is closely related to the right to privacy recognised under the *Universal Declaration of Human Rights*, Article 12 and the *International Covenant on Civil and Political Rights*, Article 17.

[16] Rechnungshof v Österreichischer Rundfunk and Others (C-465/00, C-138/01, and C-139/01) [2003] ECR I-4989

[17] A29WP together with the Working Party on Police and Justice *on the future of privacy* (2009) p.6

[18] Heisenberg (2005) p.13

[19] See Lindsay (2005) P.163

[20] Also reflected in the *Directive*, Recital 10, and Articles 8(1), 12 &14(b)

[21] (n 17) p.171

[22] A29WP *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, 1998 (WP12) p.5

This approach differs from approaches taken by third countries; for example, from the 'overwhelmingly-consequentialist'[23] approach to law making retained by the *Australian* parliament, or the US 'market-based' approach.[24]

Ultimately, the difference in approaches allows us to understand why the EU and third countries adopt varying legislative approaches to privacy protection. The difference in approaches continues, despite an apparent general recognition of the mutually beneficial outcomes of continued trade and the free flow of information – with or without 'adequate' safeguards.

### 2.2.1 The *Directive*

*Article 25*

The *Directive* is heralded as the highest standard of information privacy regulation in the world, and its framework was provided by the *Council of Europe Data Protection Convention 108* (Convention 108)[25]. However, while there is no legitimate legal basis for the *Directive* to represent a binding international standard of privacy protection in the same way that an international Treaty or Convention would, it is often confused as such in the absence of a globally binding standard in the field, and because the *Directive* confers power on the Commission to pass judgment on the level of privacy protection offered by third countries. The *Directive* is thought to have enabled the EU to establish a de facto international privacy regime, with third countries implementing similar or identical legislation for the purpose of attaining an adequacy rating.[26] To that end, the *Directive* has influenced 33 data protection laws outside of Europe.[27]

[23] As described by Lindsy (2005) p.153
[24] Ibid, pp.175-177
[25] Council of Europe Convention *on the protection of individuals with regard to automatic processing of personal data*, 1981 (ETS 108)
[26] See A29WP, *Opinion 4/2002 on the level of protection of personal data in Argentina*, 2002 (WP 63) which highlighted few 'deficiencies' as the relevant Argentian law closely reflected the *Directive's* inclusion of the content principles. See also Heisenberg (2005) p.11 & 170 for a discussion on attempts by

Article 25 (1) of the *Directive* provides that:

> The Member States shall provide that the transfer to a third country of personal data that 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.'[28]

The effect of this provision is that data may flow between all countries of the EEA to a third country found to offer an 'adequate' level of protection, without further safeguards being necessary. However, this mandatory requirement of adequacy is stronger than anything found in the OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (OECD Guidelines) or the APEC Privacy Framework (APEC Framework) – both of which were influential to the governments of Australia, the US and NZ when drafting their respective privacy protection systems.

Prima facie, the absence of the requisite level of protection may result in a hindrance to the trading capacity of a third country that does not meet the *Directive's* standard. However, the practical reality is that safeguards are required more often than not because of third countries such as Australia being considered as 'non-adequate'. Third countries such as Australia continue to rely on 'further safeguards' by contractual means, as prescribed by Article 26 (2) of the *Directive* to overcome the commercially prohibitive nature of Article 25(1) of the *Directive*.

This is despite the 'rights-based' approach asserted by the EU, as reflected in the adequacy requirement. This also means that the strength of its assertion of adequacy is slightly diminished by Article 26(2) of the *Directive* which ensures that the Commission's views on adequacy are not prohibitive to continued trade with third countries.

---

third countries, such as like Argentina and Hong Kong, to draft legislation for the purpose of an adequacy rating.

[27] Greenleaf (2012) p.74 -77

[28] The *Directive* (n1), Article 25 (1) (Author's emphasis)

*Article 26 – Derogations by Contract*

Third countries implement 'ad-hoc' solutions[29]; namely, solutions of a contractual nature as permitted by Article 26 (2) of the *Directive*, in combination with Article 26(4) of the *Directive,* to overcome 'non-adequacy' ratings, and ultimately, to continue their trade relations with EEA organisations.

Article 26(2) of the *Directive* provides that:

> […]A Member State may authorize a transfer or a set of transfers of personal data to a third country which does not ensure an adequate level of protection within the meaning of Article 25 (2), where the controller adduces adequate safeguards with respect to the protection of the privacy and fundamental rights and freedoms of individuals and as regards the exercise of the corresponding rights; such safeguards may in particular result from appropriate contractual clauses [30].

Derogations by contract as a means of regulating international transfers of personal data has its history in a study jointly conducted by the Council of Europe, the International Chamber of Commerce and the European Commission in 1992. Contractual derogations may be employed by third country organisations so long as the subject contract is drafted in such a manner as to '[…]Satisfactorily compensate for the absence of a general level of adequate protection, by including the essential elements of protection which are missing in any given particular situation'. [31] To this end, Article 26(4) of the Directive provides for the Commission to issue standard contractual clauses in accordance with the procedure laid down at Article 31 of the *Directive*.

In practical terms, when trade is conducted between the EEA organisations and those of 'non-adequate' third countries, such as Australia, the content principles and the procedural enforcement mechanisms that the A29WP consider to be missing from the third country's privacy protection system must be otherwise provided for in a service contract. For example, *Australian* organisations receiving the data of EU citizens must include in their service

[29] A29WP *Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy,* 1997 (WP4) p.1
[30] (author's emphasis)
[31] (n 22) p.16

contracts 'detailed' standards of information practices including the right to notice, consent, access, and to legal remedies.[32]

Thus, the Article 26(2) *contract derogation* is the first hint that the necessity of trade will not be compromised by the right to information privacy. Trade as a determinative of adequacy is further emphasised in the Commission's and the A29WP's adequacy assessments of the US *SHA* and the *NZ Act*. This in turn, weakens the bite of the adequacy criterion, as enunciated by the A29WP.

## 2.3 Assessing adequacy of a third country information privacy protection system

The European Council and the European Parliament confer power on the Commission to determine – on the basis of Article 25 (6) of the *Directive* – whether a third country ensures an 'adequate' level of protection for data being transferred outside of the EEA. The effect of this is that the EU is able to pass judgment on the privacy protection systems of third countries.

The Commission decides on the adequacy of third country privacy protection systems with the advisory assistance of the A29WP. In the context of assessing adequacy, the status of the A29WP is elevated from that of an advisory body, to one with more influence as the formal criterion maker and adequacy assessor. This is the result of the A29WP publishing two formal documents, the first in 1997 and the second in 1998, in an attempt to define the adequacy requirement for the purpose of Article 25(1) of the *Directive*. With the exception of the A29WP's Opinion relating to the level of protection offered under the US *SHA*, the A29WP's criterion, and its application of that criterion to third countries, has been adopted by the Commission with next to no hesitation. This has also occurred in the absence of any other guidance from the *Directive* as to the adequacy requirement, informal or otherwise.

[32] Ibid, p.17. An example of a 'contractual arrangement' may be found in the 'Inter-territorial Agreement' between the Berlin data protection commissioner and the American banking supervisory authorities, which resolved the *Citibank Bahncard dispute* cited in (n 22) pp.15 & 17; or Agreement between the EU and Australia on PNRs, 2003 [OJL 186/4]

However, it is important to remember that the criterion is non-binding and the legal legitimacy of imposing a domestic regulation extra-territorially is questionable. In that regard, there is a quiet discontent with the Commission imposing its adequacy requirement on third countries that lie beyond its legal jurisdiction:

> Some non-European countries have resented the perception that Europeans have been trying to force a particular, and narrow, approach to privacy protection on the rest of the world through the application of the transborder data flow provisions in the Directive.[33]

Ford[34] comments:

> The EC Data Protection Directive may serve well as a document for the EU but it is not an adequate basis for international agreement. It is no different in principle from the idea of Australia joining with New Zealand and Pacific Island States (assuming we could reach agreement) to settle a statement of principles and seeking to impose the result on the rest of the world.

This discontent also arises as a result of the different approaches to privacy protection taken by the EU and third countries such as Australia.

Thus, the use of 'adequate' in the *Directive* implies something far greater than the vernacular understanding of adequate as simply 'good enough'. The legal understanding of 'adequate' with reference to 'adequate grounds' as taken to mean 'reasonable' is also not relevant to the A29WP's interpretation of 'adequate'. Thus, the adequacy criterion remains inconclusive and subject to a selective and inconsistent application to the privacy protection system of a third country undergoing assessment.

Despite the problems stemming from the inconclusiveness of the criterion, the Commission maintains that determinations of adequacy remain important[35], and will continue as part of the 2015 proposed framework for data protection. In the absence of an

[33] Waters (2003) unpaginated
[34] Ford (2003) unpaginated
[35] European Commission proposal for *Data Protection Framework* for 2015: *General Data Protection Regulation* 2012/0011 (COD) Articles 40-42

alternative, the adequacy criterion as formulated by A29WP opinion are likely to remain the basis for assessing the adequacy of third country privacy protection systems.

### 2.3.1 Guidance provided by the *Directive*

The term 'adequate' in the context of Article 25(1) of the *Directive* is left undefined. The *Directive* provides limited guidance on what specific aspects of a third country's regulatory framework may be considered when assessing adequacy for the purpose of Article 25(1) of the *Directive*. The *Directive* merely provides that the Commission may make a positive finding when the protection offered by a particular country meets the adequacy requirement.[36] Conversely, the Commission may make a negative finding when the protection offered by the third country is found not to meet the adequacy requirement,[37] even though the adequacy criterion remains inconclusive. The *Directive* does, however, generally stipulate what may be taken into account when assessing the adequacy of a third country's privacy regime. Article 25 (2) of the *Directive* provides that:

> The adequacy of the level of protection afforded by a third country shall be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration shall be given to the nature of the data, the purpose and duration of the proposed processing operation or operations, the country of origin and country of final destination, the rules of law, both general and sectoral, in force in the third country in question and the professional rules and security measures which are complied with in that country.

Arguably, there was a lack of foresight regarding the practical difficulty of applying the adequacy requirement at the time of drafting Article 25(1) of the *Directive*. In fact, without A29WP opinions on the matter, the inclusion of the word 'adequate', which has necessitated laborious third country assessments, would be fraught with controversy.

[36] The *Directive* (n 1), Article 25 (6)
[37] The *Directive* (n 1), Article 26(4)

### 2.3.2 Criterion established by A29WP opinion

Although the A29WP has no explicit role in making decisions about particular data transfers[38], it assumes an elevated status when it comes to assessing the privacy protection systems of third countries because it may arrive at a provisional view of the adequacy of protection provided by third countries.[39]

Moreover, while the A29WP's adequacy criterion is outlined in its 1997 *Discussion Document*[40] and *1998 Working Document*[41] (referred to as Opinions for cohesiveness throughout this thesis), these criterion are not conclusive.

*The 1997 Opinion*

According to the A29WP 1997 Opinion, 'any meaningful analysis of adequacy must comprise two basic elements: the content of the rules applicable, and the means for ensuring effective application.'[42] The 'content principles' are viewed as a minimum requirement for protection to be considered adequate. They include:

- Purpose Limitation Principle;
- Transparency Principle;
- Security Principle;
- Rights of Access, Rectification and Opposition Principle; and
- Restrictions on Onward Transfers Principle.

Additional principles to be applied in certain circumstances include principles relating to:

- sensitive data;
- direct marketing; and

[38] This role is carried out by the Member States in the first instance, and then the Commission under the Comitology procedure laid down in the *Directive*, Article 31
[39] (n 29) p.2
[40] (n 29)
[41] (n 22)
[42] Ibid, pg.4

- automated individual decisions. [43]

However, content principles are conceptual and may be implemented by third country systems in differing ways. This may result in the A29WP overlooking the case where a third country privacy protection system achieves the overall objective of the principle but may have, for example, worded it differently to the letter of the *Directive.* Thus, the focus on the inclusion of content principles means that the surest way for a third country to attain an adequacy rating is by simply transposing the *Directive's* provisions into its own laws.

In addition to content principles, the 1997 Opinion identifies that procedural aspects of a third country's privacy protection system will support adequacy. To that end, a third country privacy protection system must include in its legislation provisions on liabilities, sanctions, remedies, supervisory authorities and notification, to the same extent that they are provided by the *Directive*[44]. This is a demanding task, considering that neither *Convention 108* nor the OECD Guidelines – influential instruments in the development of privacy protection systems in third countries – require their members to include additional mechanisms such as supervisory authorities in their privacy protection frameworks.

The A29WP states, furthermore, that it expects that the above minimum requirements be applied in a flexible enough manner to enable a 'case-by-case' approach[45]. Thus, flexibility ought to result in a finding of adequacy in privacy protection systems of third countries, even where weaknesses exist. In the same vein, flexibility ought also result in a finding of adequacy where a third country seeks to foster a high level of privacy protection, but provides for it in a variety of ways which are appropriate to its own legal, cultural and economic traditions and aspirations. As seen below, this is not always the case.

The inconclusiveness of the criterion allows the A29WP to selectively apply it at times to require something closer to equivalence[46]. Examples of third country privacy protection legislation being deemed 'adequate' by the Commission when those legislative instruments

[43] The continued validity of the content principles were recognised in the A29WP and the Working Party: (n 17)
[44] The *Directive* (n 1) Recital 32
[45] (n 29) p.1
[46] Kierkegaard et al (2011) p.230

reference almost identically the wording of the content principles found in the *Directive* include assessments of the relevant legislative instruments of Argentina[47], The Eastern Republic of Uruguay[48], Guernsey[49], and Israel[50], for example. Simply transcribing relevant provisions of the *Directive* by a third country into their privacy protection legislation may be the result of confusion as to what constitutes 'adequate' under Article 25(1) of the *Directive*.

The general confusion that ensued following the A29WP 1997 Opinion necessitated the more comprehensive 1998 Opinion, which provides a less abstract view of 'adequacy' for the purpose of Article 25(1) of the *Directive*.

*The 1998 Opinion*

The A29WP's 1998 Opinion expanded upon the 1997 Opinion to outline the more practical steps to follow when assessing the adequacy of a third country's privacy protection system.

It unequivocally states that the first step in assessing compliance with the adequacy requirement is to consider whether protection in the destination country is 'adequate' by virtue of relevant laws or effective private sector self-regulation. At this step, account ought to be taken of the relevant non-legal rules that are complied with; for example, the role of industry self-regulation.[51]

If adequacy does not become apparent on application of the first step, the second step requires a 'search' for a solution in the form of adequate safeguards, such as the contractual solutions envisaged by a combination of Article 26(2) and Article 26 (4) of the *Directive*. Here, Binding Corporate Rules are considered an appropriate solution for multinational companies to meet their legal obligations, and to ensure an adequate level of protection of

[47] (n 26)
[48] A29WP *Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruguay*, 2010 (WP177)
[49] *A29WP Opinion 5/2003 on the level of protection of personal data in Guernsey*, 2003 (WP79)
[50] A29WP *Opinion 6/2009 on the level of protection of personal data in Israel*, 2009 (WP 165)
[51] A29WP, *Opinion 7/1998 on judging industry self- regulation*, 1998 (WP7)

personal information when transferring data out of the EU. If no solution were found at this step, the third step would be to block the transfer.

Following the 1998 Opinion, therefore, the theoretical steps proposed by the A29WP in assessing adequacy are more transparent. However, this does not alleviate the problematic nature of applying the adequacy requirement in practice. This is because the criterion remains inconclusive, thereby leaving room for the inconsistent application of aspects of the three-step process. In particular, the A29WP or the Commission may selectively expand the criterion to consider self-interest factors, such as trade, as the basis of an adequacy finding.

The A29WP recognizes, furthermore, that no system can guarantee 100% compliance. It confirms that 'good systems' may be assessed as 'adequate' if they are characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights. However, data subjects must be able to enforce their rights 'rapidly and effectively' and 'without prohibitive cost'.[52] The A29WP does not elaborate, however, on what it considers to be 'rapid' and 'effective' enforcement, nor on what would amount to 'prohibitive cost' in a third county.

According to Kierkegaard et al[53] :

> The current European approaches towards transborder data flows are not working satisfactorily and are burdensome to those whose motives are benign and ineffective towards those more malignly inclined. This is notwithstanding the fact that there is a history of EU Member States inconsistently incorporating the Directive's into national law.[54]

In fact, the Commission itself expressly referred to the principle of 'subsidiarity', allowing each member state to create a law to implement the *Directive* in its own way. If the Commission chooses to accept adaptation from its own member states, it is confusing as to why it appears to require something closer to equivalence from third countries.

---

[52] (n 22) p.7
[53] (2011) p.231
[54] Directives can result in laws that are not sufficiently similar across European jurisdictions, see: The European Commission *First report on the implementation of the Data Protection Directive*, 2003 (COM/2003/0265)

However, in 2000, the Article 31 Committee[55] sought to assist the A29WP in defining 'adequate' by explaining what is not, rather than what it is: 'Adequate protection does not necessarily mean equivalent protection, and nor does it necessarily require that third countries adopt a single model of privacy protection'.[56]

It ought to be the case that if the EU wishes to impose the adequacy requirement on third country privacy protection systems, then it ought to detail precisely how that requirement can be met. Doing so would better achieve the objective of Article 25(1), namely the highest standard of protection for EU citizens' data when it is transferred to third countries, and better limit the continuation of transborder data transfers in breach of the Article 25(1) of the Directive.

There is also discontent within the EU itself as to the shortcomings of the adequacy requirement. In 2009, the A29WP, together with the Working Party for Police and Justice, agreed that it was necessary to re-design the adequacy process.[57] They also called for 'defining more precisely the criterion for reaching the legal status of adequacy'. Thus, more than ten years after its inclusion in the *Directive,* the adequacy requirement continues to cause confusion both within the EU and for third parties who are legislating with the aspiration to attain an adequacy rating. The adequacy criterion is riddled with problems that prevent effective practical application.

### 2.3.3. Other factors influencing the adequacy assessment: trade

As the 1997 and 1998 Opinions provide inconclusive and non- exhaustive criterion for adequacy, it is left open for the A29WP to take into account other factors, such as trade, to make a finding of adequacy. The problem with this is that trade considerations influence A29WP assessments and\ or the Commission's decisions regarding adequacy for a few select countries, rather than such an approach being uniformly adopted. The granting of adequacy

[55] The *Directive* (n 1) Article 31

[56] Text on Non-Discrimination adopted by the Article 31 Committee (31 May 2000), cited in D Solove, M Rotenberg and P Schwartz (2006) p.935

[57] (n 17) p.10

ratings to the US *SHA* and the *NZ Act* provide two prime examples where the Commission and the A29WP considered trade as the overwhelming element of the criterion in their respective decision and\or assessment, albeit for contrasting reasons.

*The Case of the* US *SHA (In brief)*

The Commission granted the US *SHA* adequacy status for the purpose of Article 25(1) of the *Directive* despite criticisms that it provided a less than 'adequate' level of protection to EU citizens' data citizens when their personal information was transferred from within the EEA to the US, and in the face of protests by the A29WP and the European Parliament. Thus, it has long been suspected that the decision was made on the basis of ensuring continued trade. (The US *SHA,* and the effect of the Commission's trade related leniency, will be addressed in more detail Chapter 4.2).

*The Case of NZ (In brief)*

The A29WP appears to have been mainly responsible for the Commission's emphasis on trade considerations to support the finding of adequacy in the *NZ Act*. The A29WP's Opinion that adequacy exists in the *NZ Act* was expressly made on the slim likelihood of significant amounts of EU Citizens' data being transferred to, or stored in NZ because of its isolation from Europe.

The New Zealand case shows that the position of smaller trading partners is as influential as large trading parties with respect to the question of adequacy. In other words, the weaker trading relationship between the EU and New Zealand resulted in the A29WP opining that it was less necessary for the NZ Act to be fully compliant with the *Directive*. (The case of the *NZ Act* and the effect of the A29WP's trade-related leniency will be addressed at Chapter 4.3 of this thesis).

Although trade considerations directly resulted in adequacy ratings for the US *SHA* and the *NZ Act*, the assessment of the *Australian Act* applied the criterion as enunciated by the A29WP more rigorously, and with no regard for trade considerations; close to full compliance with the *Directive* was required of the *Australian Act*.

# 3 Applying the adequacy criterion to a third country: Australia

## 3.1 Introduction

The case of Australia highlights the A29WP's inconsistent application of the adequacy criterion. Unlike the Commission's decision relating to the adequacy of the US *SHA*, and the A29WP's assessment of the *NZ Act*, the *Australian Act* was examined rigorously and with a strict application of the adequacy criterion. Furthermore, trade considerations did not feature in the assessment of the *Australian Act*. The *Australian Act* was denied an adequacy rating in 2001.

The *Australian Act* is undergoing substantive reform. Whether such reform will make Australia eligible for an adequacy rating is uncertain in light of the unpredictable outcomes of adequacy assessments resulting from variations in the criterion applied.

## 3.2 The Australian jurisdiction

The Commonwealth of Australia is a constitutional monarchy with a federal division of powers. There is no explicit constitutional right for privacy protection in Australia; however, the protection of personal information privacy under the *Australian Act*, as it applies to all States and Territories under federal jurisdiction, is derived from the express power to make laws with respect to 'external affairs' under Section 51(xxix) of the Australian Constitution[58].

The division of roles between the federal *Australian Act* and equivalent State and Territory legislation enables the latter to legislate concurrently with the federal legislature on the proviso that State and Territory Parliaments do not legislate inconsistently with the federal legislature.[59] Thus, there exists a proliferation of Commonwealth[60], State, and Territory[61]

[58] *The Commonwealth of Australia Constitution Act 1900*
[59] Ibid, s109
[60]Commonwealth laws contain specific privacy provisions including provisions relating to information about health insurance claims, data matching, information about old criminal convictions and personal information disclosed by telecommunications companies
[61] Including: *The Information Privacy Act 2000*(Vic); *The Information Act 2002*(NT); *The Information Privacy Bill 2007*(WA); *The Privacy and Personal Information Act 1998*(NSW); *The Personal*

information privacy legislation which is either directly or indirectly used for this purpose. There is however, no statutory cause for a breach of privacy[62], and nor is there a common law action for the right of Privacy in Australia.[53] However, as Australia is a common law jurisdiction, information privacy is protected indirectly through breach of privacy actions which fall under other laws, such as nuisance and trespass laws.

Due to the complications arising from a federal system, Australia falls into the category of third countries that are considered problematic when assessing the adequacy of a data protection system[63].

### 3.3 The Australian approach to information privacy legislation

Although the Australian Government purports to offer information privacy protection to its citizens generally, and in the context of cross-border transfers of personal information under the *Australian Act*, the legislative approach taken by the Australian Government differs somewhat to the approach taken by the EU.

The European approach to legislating generally differs as it is based on a deontological approach, in contrast to Australia's consequentialist approach.[64] Thus, the view held by the Australian Government (and incidentally, the OECD) is that privacy protection should not create unnecessary obstacles to cross-border flows of personal information. Australian lawmakers are willing to justify privacy legislation insofar as it produces desirable outcomes. Thus, Australia and (similarly) the US have difficulty dealing with European-born arguments that privacy rights should be respected regardless of the consequences, and with the EU purporting to assert authority extra-territorially. The socio-political differences between the

---

*Information Protection Act 2004*(Tas), *Health Records (Privacy and Access) Act 1997*(ACT); *Health Records and Information Privacy Act 2002* (NSW); *Health Records Act 2001*(Vic).

[62] The Australian Parliament may introduce a statutory cause of action for serious invasions of privacy during the second stage of reforms to the *Australian Act*. Greenleaf, Waters and Bygrave (2007) p.5 suggest that as Commonwealth has asserted constitutional power in relation to the protection of privacy in the private sector, it may be consistent for the Commonwealth to also legislate for a statutory tort to protect aspects of privacy

[63] (n 22) p.26

[64] For a summary of the differences between such approaches: Lindsay (2005)

continents are reflected in their respective information privacy protection instruments, the subject of determinations on adequacy.

In practice, the Australian federal approach to information privacy protection adopts principle-based regulation which set an overall objective. This approach is similar to the approach adopted by the European Parliament in identifying the privacy protection content principles. This principle-based approach has resulted in a framework incorporating high-level principles of general application that provide the flexibility required to take into account developing technologies, and to be more resilient to amendment and reform. According to the Australian Parliament, this approach is '[…]The best regulatory model for information privacy protection in Australia[…]'[65].

Australia can be said to innovatively recognise a co-regulatory scheme which aims at bridging the gap between legislation and self-regulation by giving self-regulation the force of law. Self-regulation was recognized by the A29WP in its 1997 and 1998 Opinions as forming part of the adequacy criterion.

Nevertheless, the A29WP concluded that a number of aspects of the *Australian Act* amounted to deficiencies in the level of privacy protection offered by the *Australian Act.* However, this was arguably the result of a strict application of the adequacy criterion to the *Australian Act.*

### 3.3.1 The *Privacy Act 1988*

Australia has had federal legislation to protect personal information in the public sector since the commencement of the *Australian Act* in 1988, which introduced the Information Privacy Principles (IPPs). The Act was amended in 2000[66] to extend the regulation of the handling of personal information to private sector organisations under the National Privacy Principles for the Fair Handling of Personal Information (NPPs). Private sector organisations

[65] Australian Parliament (2012) p.52

[66] Under the *Privacy Amendment (Private Sector) Bill 2000.* Attaining an adequacy rating was the primary motivation for reforms to the *Australian Act* in 2000 and 2004

are bound by the NPPs unless there exists a relevant privacy code approved by the Privacy Commissioner. The implementation of the *Australian Act* is overseen by the Office of the Information Commissioner.[67]

The *Australian Act* borrows some concepts from the *Directive,* but not its regulatory underpinning.[68]

The recently passed *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 (*the *2012 Bill)* provides for a single set of privacy principles called 'The Australian Privacy Principles' (APPs), and maintains Australia's principle-based approach to regulation in this area.

### 3.4 Adequacy of the *Australian Act* as previously assessed

In March 2001, the A29WP released its Opinion[69] that Australia's privacy protection system, insofar as protection under the *Australian Act* extends to the private sector, did not offer an 'adequate' level of protection for the purpose of Article 25 of the *Directive*; consequently, additional safeguards are required for the transfer of personal information from within the EU to Australian organisations.

In a strict application of the adequacy criterion, the A29WP considered that the major barriers to Australia attaining an adequacy rating are the inclusion of the Small Business Exemption (SB Exemption) and Employee Records Exemption (ER Exemption) in the *Australian Act*. The A29WP also opined that that the principle-based requirement at the (then) NPP9 offered only 'weak' protection for onward transfers of personal information. These are the subject of current reform.

[67] A member of the Human Rights and Equal Opportunity Commission, established as a separate statutory agency in 2000.
[68] Ford (2003) unpaginated
[69] A29WP *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000*, 2001 (WP40)

There were other barriers[70] to a finding of adequacy in relation to the *Australian Act.* The A29WP took issue with the *Australian Act's* provision relating to access to publicly available information. This opinion dismissed the Australian Parliament's view that 'right of access' need not be considered after the material has been made publicly available because it is accessible on the basis that it is already publicly available. This view is held because, prior to the collection of the publicly available material, NPPs 1 (Collection), 2 (Use and Disclosure) and 3 (Data Quality) have already been complied with.

The A29WP also misinterpreted the Australian approach to 'sensitive information', which is always subject to the NPPs at the first stage of collection; this precludes further treatment by the NPPs at the latter stages of processing and disclosure.

Another misreading of the *Australian Act* by the A29WP is seen in relation to the protection of personal information in the context of Direct Marketing. However, this issue is best dealt with below when we consider the ways in which the Commission took a more lenient approach to finding adequacy in the US *SHA.*

This thesis will examine in more detail the major barriers to adequacy, namely the SB Exemption and ER Exemption and the transborder transfer provision.

## 3.5 Addressing issues of contention between Australia and the EU

Given the large number of 297 recommended reforms proposed by the ALRC, the implementation of these reforms is a two-stage process. The first stage of reform was implemented by way of the *2012 Bill.*[71]

The first stage of reforms repeal the previous NPPs and IPPs as they applied separately to government agencies and to private organisations in favour of the uniformly applicable Australian Privacy Principles (APPs). APP8 now refers to the 'Cross-Border Disclosure' of Personal Information, the *Australian* equivalent to the EU's transborder transfer principle.

[70] Ford (2003) provides a more detailed discussion of the other 'barriers' mentioned here
[71] The *2012 Bill* was introduced into the House of Representatives on 23 may 2012. It received royal assent on 12 December 2012. The reforms come into force on or around March 2014.

The second stage of reform, to be delivered on a yet unspecified date, will address the proposed removal of the SB Exemption [72] and the ER Exemption [73], as well as the development and publication of a list of laws and binding schemes that effectively uphold principles for the fair handling of personal information. (The latter refers to APP8, discussed at 3.5.3

### 3.5.1 The small business exemption

The SB Exemption (which extended in application to nonprofit organisations) was introduced in the 2000 amendments. For the purpose of the *Australian Act*, Small Businesses include businesses which: have an annual turnover of 3 million (AUD) or less; which provide a health service; which collect personal information from third parties and disclose such information for a benefit, service or advantage without obtaining the individual's consent; or businesses which are contracted to provide a service to the Commonwealth.[74]

The A29WP raised issues concerning the complexity of the exemption and, in turn, with the inability (in its view) to determine which businesses might fall within the scope of the provision. The A29WP thus determined that that it would be necessary to assume that all data transfers to Australian businesses would potentially be made to a small business operator and, therefore, would not be subject to the law.

The *Australian Act* did not exempt all businesses from complying with the Act. Small businesses lose their exemption as small business operators if, amongst other things, they collect or disclose personal information for a consideration.[75] Others not permitted to take advantage of the SB Exemption were, for example, small health service providers handling 'sensitive' personal information. Ford[76]recognises that the A29WP did not well understand this aspect of the *Australian Act*, and that '[…]The assumption should be that businesses are covered, not the reverse.' The exemption, of course, would be businesses that rarely deal

[72] ALRC Report 108 (2008) Recommendation 39
[73] Ibid, Recommendation 40
[74] Previously set out in the *Australian Act*, s6D
[75] The *Australian Act*, Section 6D(4)
[76] (2003) unpaginated

with personal information (such as local butchers and the like) and which, on that basis, should fall within the SB Exemption.

Irrespective of this, the fact that no comparable jurisdiction in the world exempts small businesses in the same way was reason enough for the A29WP to cite this exemption as 'unusual' and, as such, a major obstacle to the *Australian Act* being granted adequacy status in 2001. Thus, the *Australian* Government's right to self-determine this aspect of its legislation in light of the socio-political milieu in which that legislation operates was not recognised by the EU.

*The Proposed Reform*

The SB Exemption is the subject of proposed reform. The ALRC recommends its removal, as do Australian privacy advocates[77].

Subject of course to political partisan preference, it is likely that the Australian Parliament will adopt the ALRC's recommendation, and remove this barrier to a finding of adequacy.

### 3.5.2 The employee records exemption

Section 7B of the *Australian Act* contains an exemption for some employee records in the private sector[78], on the grounds that such matters are more appropriately dealt with by workplace relations law[79]. Practical examples of personal information relating to an individual's employment may include: the engagement, training, disciplining or resignation of the employee; the termination of employment; and the terms and conditions of employment. However, this exemption is limited to acts such as the 'processing', and to 'practices directly related to current and former employment relationships'[80]. What this

[77] Greenleaf, G et al (2012) 113
[78] The term 'employee record' is defined broadly at s6(1) as '..a record of personal information relating to the employment of the employee.'
[79] Australian Parliament *Second Reading Speech* Hansard 12.4.200, p 15752
[80] *Australian Act,* s7B(3) (a- b)

means is that prospective employment relationships are likely to be considered not to fall within the intended scope of this exemption. On the other hand, the public sector has always been required to treat ERs under the IPPs.

In contention with the ER Exemption, the A29WP opined that employee data is 'sensitive information' and should therefore be given greater protection, rather than be excluded. The A29WP also and wrongly assumed that ERs might be disclosed to a prospective employer. This contradicts the Australian view, and reflects a misreading of the *Australian Act.*[81] The Australian Government contends that the A29WP's concerns with the ER Exemption rest on a misconception of the exemption, and that the prospective employer would always have to comply with the collection principle and notify the individual of the collection.[82]

Thus, in its strict application of the adequacy criterion, the A29WP has failed to consider the practical effects of this aspect of the *Australian Act.*

*The Proposed Reform*

The ALRC have proposed the removal of the ER Exemption in the second stage of reforms. As is the case for the SB Exemption, there is opposition to retaining the ER Exemption amongst privacy advocates within Australia, who fear that it creates 'privacy-free zones'.[83]

However, despite it recommending the removal of the ER Exemption, the ALRC also acknowledges that there remain certain situations in which it is undesirable for employees to have access to their records, reviews and other similarly confidential information.

While there exists a likelihood of the Australian Parliament adopting the proposed removal of the ER Exemption from the *Australian Act*, there is also some chance that it will maintain that employee records ought to be dealt with under industrial relations law, or on the basis of the general common law of confidentiality.

[81] Ford (2003) unpaginated
[82] Ibid
[83] Greenleaf, Waters & Bygrave (2007) pp.11&58

### 3.5.3 The 'weak' protection of onward transfers

NPP9 prohibited the export of personal information by an organisation[84] to someone in a foreign country (other than an affiliate of the organisation itself) unless one of six conditions applies. One such condition[85] provides that an organisation in Australia (or an external Territory) may transfer personal information about an individual to someone who is in a foreign country, if the organisation 'reasonably believes' that the recipient of the information is subject to a law, binding scheme or contract which effectively upholds principles for fair handling of the information, and which are 'substantially similar' to the NPPs. This condition was the basis for the A29WP's observation that Australia provided merely 'weak' protection in the instance of transborder data transfers. However, the A29WP's opinion was heavily influenced by the fact that The *Australian Act* did not explicitly legislate for non-Australian data; namely, the personal data of EU citizens (the Australian Parliament reformed this in 2004).

Where the *Directive* requires that the protection offered by a third country be 'adequate' for the purpose of data transfers, the *Australian Act* requires that the third country upholds principles for fair handling of the information that are 'substantially similar' to the NPPs. On a basic level, therefore, some aspects of the contention appear to be based in semantics. In this regard, it is difficult to understand there to be an overwhelming difference between the descriptors 'adequate', as employed by the *Directive,* and 'substantially similar', as used in the *Australian Act*. Nevertheless, the A29WP opined that NPP9 has the effect of circumventing the EU *Directive.* In addition, the inclusion of 'reasonably believes' in the contentious condition led A29WP to interpret NPP9 as allowing an Australian company to import data of EU citizens and subsequently export it to a country with no privacy laws.

The A29WP left little room for the Australian Government to include in its own legislation language that is characteristic of its own legal tradition. It also allowed little flexibility for consideration of the region in which Australia operates; for example, the diversity of members in APEC makes it more complicated than it appears to impose

[84] As defined by the *Australian Act,* s6C
[85] The *Australian Act,* NPP9 a)

prescriptive requirements for the protection of information privacy in a carte blanche manner. Requiring a uniformity of laws when few governments in the region have information privacy laws of greater strength than that recommended in the APEC Framework can jeopardise the Australian Government's relationships with its neighbourhood trading partners.

Additionally, the Australian approach to cross-border transfers may represent the same approach taken by APEC - an approach which Tan[86] considers to be a more pragmatic facilitation of e-commerce, rather than a rights-based European model.

Ultimately, while the Australian approach to the protection of personal data in the context of transborder transfers differs from the approach taken under the *Directive*, it is suggested that it is not significantly weaker. According to Ford[87]:

The Australian law on transborder data flow follows that of the Directive but also adds another provision allowing transfers when the organisation has taken reasonable steps to ensure that the information which it has transferred will not be held, used or disclosed by the recipient of the information inconsistently with the National Privacy Principles.

It would seem, then, that the A29WP took a particularly tough stance against NPP9, especially in light of its own inability to conclusively define the adequacy requirement.

*Proposed reform*

The Australian Parliament appears uncompelled to significantly reform its privacy principle relating to cross-border data transfers for the sole purpose of attaining an adequacy rating.

The wording of the contentious condition at NPP9 was only slightly reformed. APP8 includes the phrase 'at least' before 'substantially similar', and now requires mechanisms

[86] Tan (2008) p.20. Also see: Svantesson (2010) for a discussion on how Australia proposes to regulate privacy protection in transborder data transfers
[87] 2003 (unpaginated)

that the individual can access to take action to enforce the protection of the law or binding scheme.[88]

### 3.6 What the EU missed: overlooking parts of the *Australian Act,* and influencing attitudes to adequacy

The A29WP's rigid assessment of the *Australian Act* resulted in additional protection offered under the *Australian Act* being overlooked. This in turn, may influence the Australian Government's attitude to the adequacy requirement.

The A29WP's focus on the SB and ER Exemptions, and the onward transfer principle means that they overlooked the Australian Government's incorporation of two additional privacy principles relating to anonymity and the use of identifiers: the 'Anonymity Principle', which requires that wherever lawful or practicable, individuals must have the option of not identifying themselves when entering into transactions with an organization; and the 'Identifiers Principle', which limits the right of an organisation to adopt as its own an identifier of an individual that has been assigned by a government agency, for example, a Tax File Number[89]. Ford[90] opines that if:

> […]The Article 29 Opinion is based on a view that, rather than focus on a comparative assessment of particular issues, there should be an overall assessment of a country's privacy protection, it follows that there should be some flexibility…It may be that the level of privacy protection departs from the Directive's standards on some issues, but on other issues the level of protection may be higher than in Europe or than in another country with an 'adequacy' rating (for example, Australia's additional NPPs).

In light of the A29WP's strict approach to assessing the *Australian Act* and its tendency to misunderstand the effect of some Sections of Australian Law, the simple removal of barriers to adequacy does not guarantee an adequacy rating for the *Australian Act.* Any reluctance to implement regulatory reform for the purpose of attaining an adequacy rating is likely

[88] The *2012 Bill*, APP8.2 a) i) and ii)
[89] An Australian Tax File Number is given to individuals and organisations to help the Australian Government administer tax and other Australian Government systems
[90] (n 76)

exacerbated by the A29WP's and the Commission's inconsistent application of what is an inconclusive adequacy requirement that has resulted in more favourable treatment of other third countries' privacy protection systems, such as the US *SHA* and the *NZ Act*.

# 4 Applying the adequacy criterion to analogous third countries

## 4.1 Introduction

While the level of protection offered by the *Australian Act* was deemed not adequate on an arguably rigid application of the adequacy criterion, privacy protection instruments of third countries of analogous jurisdiction to Australia have received adequacy ratings. In this regard, the adequacy criterion was selectively altered to include trade relations when they may be jeopardised by the finding of non-adequacy – which resulted in the approval of the US *SHA* – or conversely, when there is a minimal trade relationship that limits the prospect of abuse of the personal data of EU citizens when data is unlikely to be transferred to, or stored in the third country. This latter consideration was the premise for the A29WP Opinion of the adequacy of the *NZ Act*.

For the purpose of this thesis, 'analogous jurisdiction\s' are countries which have similar legal traditions; in this case, Australia, New Zealand, and the US. These similar traditions largely stem from their respective histories as British colonies. In fact, the Australian legal system is said to be a hybrid of the British and the US systems[91]: Australia and the US are both federal nations with written constitutions; New Zealand is a unitary state with Parliamentary sovereignty; and New Zealand, the US, and Australia adhere to secular common law legal systems which acknowledge the rule of law and the separation of powers. Apart from these legal similarities, the term 'analogous jurisdiction\s' also loosely reflects the similar socio-political and cultural aspects of these three countries.[92]

## 4.2 US case study: avoiding the adequacy requirement to protect trading interests

The decision to find adequacy in the US *SHA* epitomises the situation where regulating privacy is compromised by the need to facilitate commerce. In 2000, the Commission and the

[91] Coper (2007) p.1
[92] The scope of this thesis does not extend to a more thorough discussion of such similarities

United States Department of Commerce (US DOC) reached a compromise regarding the adequacy requirement when they entered into the *SHA*.

The Safe Harbour Principles were issued by the US DOC, together with a set of Frequently Asked Questions (FAQs); together, these were meant to reflect the minimum requirements for adequacy, namely, the EU content principles and procedural mechanisms to effect enforcement. However, the US *SHA* is said to be an agreement that enabled transatlantic data (and hence commerce) to flow, despite not meeting the letter or intent of the *Directive*.[93]

The US *SHA* is generally accepted as falling short of adequacy. While the A29WP and the European Parliament recognised this[94], the Commission decided nevertheless that the US *SHA* was adequate for the purpose of Article 25(1) of the *Directive*. It is thus suggested that the only reason that the US *SHA* was deemed 'adequate' and exists today is because the A29WP or the European Parliament had no power to prevent the Commission from recognizing the US *SHA*.[95]

It is accepted that although it may have prevented abuses of EU citizens' personal data in some instances, the real effect of the *SHA* was to prevent the prospective blocking of data transfers and, subsequently, an estimated 120 billion (USD) worth of transatlantic commerce between the EU and the US.[96]

In the case of the US, the EU accepted that the US would not stray from its market-consequentialist approach to regulating privacy. The US privacy protection system assumes that data collection is acceptable, and potentially beneficial; thus, legislation is deemed necessary only where individual problems highlight a more fundamental problem in society. This market-consequentialist approach[97] to law making is similar to the approach taken by the Australian Parliament; however, the Australian Parliament arguably provided a more

[93] Heisenberg (2005) p.11
[94] The European Parliament voted 279 to 259 against considering the SHA adequate.
[95] Heisenberg (2005) p.8
[96] Ibid, p.4
[97] For a discussion on the US approach to privacy protection see: Lindsay (2005)

comprehensive privacy protection framework in the form of the *Australian Act,* than that which was provided by the US *SHA*.

With reference to the final version of the *SHA*, it is suggested that it appears to have been a victory for the US commercial interests that were actively involved in preventing European style regulations in the US, and that it was overall closer to the preferences of the US than those of the EU. [98]

The US policy commitment to self-regulation produced a non-mandatory *SHA*, applicable only to those private organisations who subscribe to the *SHA* principles. For those that did not, standard contractual clauses are used under Article 26(4) of the *Directive*.

There is much literature devoted to the EU and US *SHA* dispute, and trade as the basis for the agreement is a not a new conclusion. [99] This thesis only focuses on that conclusion to the extent that it highlights the leniency afforded to one third country (the US), but not another (Australia), with respect to determining adequacy. This, in turn, raises questions about the consistency of the application of the adequacy requirement.

### 4.2.1 The non-adequate US *SHA*

The US *SHA* has been the subject of much criticism due to its apparent weak protection of information privacy.

Initially, it was criticised for lacking enforcement mechanisms. In its Opinions, the A29WP explicitly require third country privacy protection systems to have enforcement mechanisms as a pre-requisite to adequacy.

The supposedly 'adequate' *SHA* allowed US organisations to adhere to the *SHA* Principles, subject to limitations posed by any 'statute, government regulation or case law'[100] without any further qualification. Furthermore, the A29WP recognised the *SHA*'s heavy reliance on

[98] Heisenberg (2005) p.4
[99] See for example Heisenberg (2005), Newman (2004), Ewing (2002), Shaffer (2000), and Mattli, W and T Buthe (2003)
[100] *SHA Principles*, Paragraph 5B

self-certification (FAQ 6) and self-assessment (FAQ 7) as a means of complying with the *SHA*.[101] While the adequacy criterion recognises self-regulation, the minimum requirements of the content principles and the procedural and enforcement mechanisms are still required. Thus, self-regulation cannot take the place of the 'minimum requirements', except with the case with the US *SHA.* Self-regulatory measures were not considered 'adequate' with the case of the *Australian Act.*

A comparison between the level of protection afforded under the *SHA* and under the *Australian Act* where Direct Marketing is concerned further highlights the inconsistency of application of the adequacy criterion. In that regard, FAQ 12, regarding the Choice Principle, permits the collection of information for the primary purpose of Direct Marketing without first obtaining consent of the data subject. The timing of the 'opt-out' choice is consequently delayed.

In contrast, under the *Australian Act,* organisations have one opportunity to directly market to consumers, but must include in that opportunity the possibility for data subjects to 'opt-out' of such marketing activities. This delay was considered to be not-adequate.

Another example of inconsistent application of the adequacy criterion relates to notifying a data subject of the collection of their personal information. FAQ 15 provides that: 'It is generally not necessary to apply the Notice, Choice and Onward Transfer Principles to publicly available information unless the European-fervour indicates that such information is subject to restrictions that require the application of those Principles.'

In contrast, the A29WP took issue with the *Australian Act* Collection Principle (NPP 1) which allows organisations to notify individuals before, or at the time of collection, but also adds that if this is not practicable, it may inform individuals as soon as practicable thereafter. The A29WP criticised this on the basis of a departure from its privacy principles, noting how this may affect a situation involving 'sensitive information'. In doing so, it disregarded the effect of NPP10, which requires consent for the collection of 'sensitive information', except in very limited circumstances.

[101] (n 5)

In relation to this issue, Ewing[102] gives a more specific critique:

> The Safe Harbour Principles do not match the breadth and depth of the Data Protection Directive. They replace the Directive's principles of limited collection and use as a fundamental right with an 'opt-out' provision, the data subject is granted a lower degree of control over his personal data. The 'opt-in' provision for 'sensitive' data is weakened by limits on the provision of an 'opt-in' choice for certain categories of sensitive data…Compared with the broad rights of access granted by the Directive in Article 11, the access rights promulgated by the Safe Harbour fall short.

In relation to onward transfers, another issue of contention between the EU and Australia, the US *SHA* relieves organisations of liability when information is transferred to certain third parties, because the data subject is unlikely to access legal redress against the transferor who may have acted recklessly. However, this was an issue for the A29WP when it assessed the equivalent level of protection afforded by the *Australian Act*

The Commission also dismissed the fact that not all employee records are fully protected by the *SHA*, while the ER Exemption was a major barrier to Australia being granted an adequacy rating.

The US *SHA* presents a no more comprehensive privacy protection system than that provided by the *Australian Act.* Ford [103] supports this view in his clear charge of discrimination against the *Directive*:

> In our view, we have also been treated differently from the US....It is possible under the Safe Harbour Principles for US companies to disregard the Directive in relation to generally available publications that contain only US data. No such principle has been recognised for Australia. We understand the concern to ensure that the Directive's standard of protection in relation to particular issues is not progressively downgraded through negotiations with other countries, but it should not result in different treatment for different countries on issues of detail of this kind.

[102] Ewing (2002) p.336
[103] (2003) unpaginated

Indeed, the weakness of the US *SHA* is well documented in the literature. Greenleaf[104], for example, comments that, 'In comparison with most information privacy laws, the six principles in the 'SHA' proposed were very weak protection.' Lindsay[105] is clearly of the same view: 'Despite the extent to which EU policy documents make it clear that the 'adequacy' requirement is intended to promote a higher level of protection than the baseline OECD Guidelines, it is clear that the Safe Harbour Principles go no further than the Guidelines.'

Waters[106] is clear in his claim that: 'The decision on Safe Harbour was widely seen as a pragmatic concession to the economic and political power of the US, since the scheme meets only a few of the criterion for adequacy set out by the Commission.'

There is much opinion, therefore, to support the suggestion that the granting of adequacy in relation to the US *SHA* undermines the adequacy requirement, the criterion of which was more strictly applied to the *Australian Act.* Specifically, decisions on adequacy are selectively based on trade power of the third country being assessed.

### 4.2.2 Conclusion: the supremacy of trade considerations

The trading capacity of the US forced the EU to ultimately accept a standard of data protection that it would not otherwise deem to be 'adequate'; in fact, the consideration of trade overrode the application of the adequacy criterion.

Thus, while it appears that the Commission was more eager to find adequacy in the US *SHA* because the US was the EU's biggest trading partner, we can assume that, in contrast, Australia did not present 'effective market power'[107] to secure an adequacy rating, and\ or to warrant a dispute between the Commission and the A29WP. However, the issue is that the

[104] (2000) p.5
[105] (2005) p.175
[106] (2003) unpaginated
[107] According to Heisenberg (2005) p.7: effective market power is a nation's capacity to deploy domestic political institutions into international political influence and provides justification for the Commission's acceptance of the less than adequate SHA.

trade power of a third country ought not to be relevant to a finding of adequacy, and the adequacy criterion ought to be applied to all third countries in the same manner.

Thus, the Commission signaled to the A29WP, and indeed to third countries seeking adequacy ratings, that trade is selectively considered an important element of the adequacy criterion.

### 4.3 New Zealand case study: insufficient trade for adequacy concerns

The finding of adequacy in the NZ *Act* is another example of trade considerations overriding a strict application of the adequacy criterion in relation to third countries other than Australia. However, the reason for the adequacy decision with respect to the *NZ Act* is in contrast to the reason for the adequacy decision in the case of the US *SHA.* New Zealand holds a minimal trading relationship with the EU; it was deemed, as a result, that there is insufficient trade transfer between the two to create a significant threat to the personal data of EU citizens. This resulted in the A29WP being less concerned with a strict application of adequacy criterion to the *NZ Act*; rather, a more pragmatic approach to determining adequacy was adopted.[108] This is again indicative of the A29WP adopting the Commission's preferential treatment of countries on the basis of trade considerations, and highlights a shift in the adequacy criterion.

While a previous assessment of New Zealand's privacy protection system focused on missing key features such as 'onward transfer provisions and coverage of non-New Zealand residents, the recent decision focused more on pragmatic considerations, such as New Zealand's geographic and economic isolation from the EU.[109]

The legislative situation in New Zealand differs only slightly to that in Australia, in that there is one main federal data protection legislation, known as the Privacy Act 1993 (as amended to include the *Privacy (Cross-Border Information) Amendment Act*); the formulation of this legislation was heavily influenced by the 1980 OECD Guidelines. The

[108] First recognised by Greeneleaf, G & Lee Bygrave (2012)
[109] Ibid

New Zealand federal privacy protection system also comprises three full privacy codes of practice under Section 46 of the *NZ Act* that apply specifically, and with more stringent standards, to health information, telecommunications information, and credit reporting information. New Zealand also boasts additional laws and related privacy legislation.[110] There also exist a number of common law principles and rules relevant to data protection including the recognition of the common law tort for privacy as well as breach of confidence.

Nevertheless, the New Zealand approach is closer to the rights-based European approach. This similarity, perhaps, made the *New Zealand Act* more accessible and favourable to the A29WP, thus influencing their assessment.

While the *NZ Act* may well have been found to offer an 'adequate' level of protection on its merits, the A29WP's opinion was, nevertheless, consumed by the likelihood of EU citizens' data being transferred to, or stored in, New Zealand. Ultimately, therefore, New Zealand's geographic and economic isolation from the EU meant that the A29WP was less bothered by the adequacy compliance of the *NZ Act*.

### 4.3.1 The *NZ Act*: deficiencies are irrelevant

Despite the comprehensiveness of the *NZ Act*, it also presented identifiable deficiencies which may have resulted in a finding of non-adequacy, had the adequacy criterion been as strictly applied to it, as it was to the *Australian Act*.

The A29WP found, for example, seven instances of 'non-adequacy' in the *NZ Act.* Such deficiencies related to the content principles. Here we recall that the A29WP, in its 1997 and

[110] The *Official Information Act 1982* covers central government and public sector agencies, and the *Local Government Official Information and Meetings Act 1987* covers local government. These include privacy provisions for when government information is proposed to be disclosed. Other related laws include spam, criminal law sanctions for certain breaches of privacy, spent criminal convictions, surveillance, the retention of health information, public records, and discrimination law. There are also privacy related provisions in other legislation for example, secrecy provisions in the *Electoral Act 1993* that protect the privacy of the voter.

1998 Opinions, stipulated that the inclusion of such content principles was a minimum requirement for an adequacy finding.

Specifically, the A29WP found that the *NZ Act's* data transfer principle did not fully comply with that of the EU. We recall further, however, that the 'weak' protection offered by the *Australian* Act was a major barrier to Australia attaining an adequacy rating. Under the *NZ Act*, there is no explicit principle for the transborder data transfers, although Section 10 deals with the application of the content principles to information held overseas. Further, the *NZ Act* enables the NZ Privacy Commissioner to issue transfer prohibitions if the recipient country does not offer 'comparable' safeguards.[111] How 'comparable' safeguards can be considered so semantically and conceptually dissimilar to the *Australian Act's* 'substantially similar' safeguards is, indeed, mystifying.

The other areas of concern for the A29WP included: the lack of a Transparency Principle (requiring that people are informed of the reason for the data being collected); the lack of the Right of Opposition; the lack of an 'opt-out' requirement for data subjects; and the inclusion of exceptions that had no corresponding exception in the *Directive.*

However, irrespective of any of these deficiencies found in the *NZ Act*, the A29WP readily found that the *NZ Act* provided an adequate standard of data protection. New Zealand was therefore considered a 'safe place' for the processing of personal data. This 'safe place' determination, however, was made on the basis that, 'given the geographical isolation of New Zealand from Europe, its size and the nature of its economy, it is unlikely that New Zealand agencies will have any business interest in sending significant volumes of EU-sourced data to third countries'.[112] This blatant admission to New Zealand's trading position being a determinative of adequacy, amounts to an equally blatant admission of inconsistent application of the adequacy criterion to the *NZ Act* and the *Australian Act.*

[111] *NZ Act, s114B*
[112] A29WP *Opinion 11/2011 on the level of protection of personal data in New Zealand,* adopted on 4 April 2011 (WP182)

### 4.3.2 The adequacy requirement: inclusion of new considerations

As evidenced above, the A29WP's Opinion in relation to the NZ federal privacy protection system places little focus on the deficiencies found in the system, and favours a focus on a more pragmatic trade-based reasoning for its adequacy finding. To that end, the A29WP gives much weight to the limited amount of trade[113] between NZ and Europe, and subsequently, to the reduced likelihood of significant volumes of EU data being transferred to, or stored, in New Zealand.

The A29WP seems to have disregarded the legislative content of the *NZ Act* per se; rather, it has decided that it is more relevant that:

> '[…]New Zealand is a small country of approximately 4.3 million people and as the expert report makes clear fair information handling is seen as good business. Organisations cannot afford to alienate such a small market, and news of poor practice spreads quickly. This has a significant effect on business practice*'.*[114]

Notably, the Opinion simply accepts that market force will play a role in the protection of personal data. The Opinion makes no allowance for any possible, future change to New Zealand's economic milieu; indeed, the A29WP's assessment will be shown to have been misguided if New Zealand does, in fact, become a favoured destination for data export and storage.

Greenleaf and Bygrave[115] opine that the position of the Commission regarding New Zealand reflects a more pragmatic rather than formalist approach that may have previously been applied; it, thus, represents a shift from the strict application of the adequacy criterion to the *Australian Act* to one entrenched in pragmatism. More specifically, Greenleaf and Bygrave suggest that '[…]Adequacy is in inverse proportion to proximity including economic and social proximity, not just geographical'.[116]

---

[113] The total trade between the EU and NZ amounts to 6.7billion Euros a year, of which 3.1billion relate to trade services: New Zealand Office of the Privacy Commissioner (2012)
[114] (n 112*)* p.3
[115] (2011)
[116] Ibid, p.3

In line with that observations, this thesis suggests that the A29WP have added a new element to the adequacy criterion; namely, geographic and economic isolation The author suggests that upon examination of the A29WP opinions regarding the *Australian Act* (to which it more strictly applied the formal adequacy criterion) and the *NZ Act* (to which it was less strict in its approach and more pragmatically flexible), the A29WP has adopted the Commission's preference for adequacy to reflect trade considerations, rather than the strict application of adequacy principles to particular privacy protection systems.

### 4.3.3 Conclusion: the game-changing New Zealand assessment

The effect of the A29WP's assessment of the *NZ Act* is a game changer where assessing adequacy is concerned. The A29WP has shown that it is willing to toe the line of the Commission, and selectively expand the adequacy criterion to include a consideration of the trading relationship between the EU and a third country. Thus, the A29WP may make future assessments based on pragmatic factors, regardless of any deficiencies in the privacy protection system of a third country that would otherwise – under a stricter application of the criterion (as was the case with Australia) – result in a finding of non-adequacy. This both further discredits the already inconclusive approach to assessing adequacy, and undermines the high standard of information privacy protection required by Article 25 of the *Directive*.

## 4.4 Summary

Overall, the trade-based adequacy findings in the US *SHA* and the *NZ Act* raises questions about the inconsistent application of the adequacy criterion to Australia. The inconsistency of application is not a new observation[117]; however, it has not yet been considered whether the inconsistency of application of the adequacy criterion constitutes discriminatory treatment of a third country's privacy protection instrument in light of Article XIV of the *Gats* as discussed at Chapter 5.

[117] Ford (2003) unpaginated

# 5 Implications of the inconsistent application of the adequacy criterion under Article XIV of the *Gats*

## 5.1 Introduction

Legitimate regulations aimed at improving the quality of electronically supplied services, such as transborder data transfers, are promoted under the *Gats*. The EU, the US, New Zealand and Australia are all Members of the WTO and parties to the *Gats*. Generally, the *Gats* applies to *measures* affecting trade in services.[118] Electronic commerce is recognised as a 'cross-border' trade in service.[119] Transborder transfers of personal data, contemplated by Article 25(1) of the *Directive*, represent a digitalised information service, and thus meet the WTO definition of 'e-commerce', namely: 'the production, distribution, marketing, sale or delivery of goods and services by electronic means'.[120]

Privacy issues have not yet been topical in WTO dispute settlement proceedings; nor has there been much academic comment on privacy legislation under the *Gats*.[121] This may be because WTO Members are said to be generally reluctant to commence proceedings pursuant to the *Gats*[122], or because all privacy protection *measures* are thought to be permissible under the Article XIV c) ii) exception of the *Gats*. This exception exempts a WTO Member from all other *Gats* commitments, including the Most-Favoured-Nation Treatment Obligation at Article II, and the National Treatment obligation at Article XVII.[123] However, to qualify for the privacy protection exception, a *measure* taken by a WTO Member must also satisfy the requirements of the *Chapeau* at Article XIV of the *Gats* by avoiding measures that are

[118] Trade in services under the *GATS* encompasses four well-known 'Modes' by which services can be supplied. *Cross-border supply* is listed at Mode 1. For a discussion on the *GATS* 'Modes' see: Weber (2010) p.8
[119] WTO S/L/74 (1999) para.4. See also Panel Report *China-measures affecting trading rights and distribution services for certain publications and audiovisual entertainment products*, WT/DS363/R adopted on 12 August 2009 (*China – AVHE*); and Appellate Body Report *US-measures affecting the cross-border supply of gambling and betting services,* WT/DS285/AB/R adopted on 7 April 2005
[120] WT/L/274 adopted on 30 September 1998
[121] Aside from articles by Weber, Rolf. (2010) and (2012), Shin-Yi Peng (2005), Wunsch-Vincent (2006), and Pauwelyn (2005)
[122] Wunsch-Vincent (2005) p.319
[123] *GATS* Scheduling Guidelines 2001, para.20

'arbitrary' or that constitute 'unjustifiable discrimination' between countries 'where like conditions prevail'.

The purpose of this chapter is to assess whether Article 25(1) of the *Directive* is a provisionally justified *measure* in light of the Article XIV c) ii) exception for privacy related *measures*. It will then be assessed whether, despite that exception, the subsequent application of the adequacy requirement (and its criterion) that resulted in in the granting of adequacy ratings to the US *SHA* and the *NZ Act*, despite obvious deficiencies – the same deficiencies which, to some extent, resulted in a finding of non-adequacy in the *Australia Act* – may still constitute a WTO-inconsistent *measure* based on the *Chapeau* at Article XIV of the *Gats*.

## 5.2 Article XIV framework

*Measures*, such as the adequacy requirement, applied in the protection of privacy are identified as regulations likely to be permissible under Article XIV c) ii) of the *Gats*, because privacy protection is considered a permissible public policy objective.

The case of the US-*Measures Affecting the Cross-Border Supply of Gambling and Betting Services*[124] (*US-Gambling*) was the first WTO dispute settlement body's judgment directly relating to the Internet, and the second only case which centred exclusively on the *Gats*.[125] It was also the first case to invoke and clarify exceptions at Article XIV, although the exception considered related to measures seeking to uphold public morals and public order.[126]

The adjudicatory arms of the WTO – the Panel and the Appellate Body – ordinarily determine cases of justified discrimination. To date, however, they have not considered privacy protection measures under the Article XIV c) ii) exception. Thus, the reasoning applied by the Panel and the Appellate Body in US-*Gambling* will be used here in an

[124] *US- Gambling* (n 119) para.292
[125] The first case centred on the *GATS*: Panel Report *Mexico- measures affecting telecommunications services* WT/DS204/R adopted on 2 April 2004
[126] The *Gats* 1994, Article XIV a)

analysis of whether the adequacy requirement, and the inconsistent application of the adequacy criterion, may be permitted under Article XIV of the *Gats*.

The relevant parts of the text at Article XIV c) ii) are:

> *Chapeau*: 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 […] [127] 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

In line with the WTO Appellate Body decision in US-*Gambling*, a 'two-tier' analysis can be used to determine whether Article 25(1) of the *Directive* is a WTO-consistent *measure*. In such a determination under the *Gats*, the adjudicatory arms of the WTO borrow the approach used to determine disputes relating to Article XX of the WTO *General Agreement on Tariffs and Trade 1948* (modified in 1994). Applying the 'two-tier' analysis to the adequacy requirement involves, first, a determination of whether Article 25(1) of the Directive is provisionally justified under Article XIV c) ii) of the *Gats*, and second, whether Article 25(1) meets the requirements of the *Chapeau.*

Preliminarily, it must be considered how the *measure* relates to the interest mentioned in the exception at Article XIV c) ii) of the *Gats*. There must be a sufficient nexus, or 'degree

[127] It also includes a third standard of 'disguised restriction on trade'. This is not considered here in light of the *Directive's* provision for the *contract derogation* to enable continued trade. Thus, it is not alleged that the adequacy requirement represents a 'disguised restriction on trade'.

of connection'[128] between the Article 25(1) *measure,* as specified in the language of Article XIV c) ii) of the *Gats*, through the use of the terms 'relating to' and 'necessary to'.

The next step is to assess the following factors to determine whether a measure is '[…]Necessary to secure compliance with laws and regulations[…]' at Article XIV c):

- the importance of the interests and values that the challenged measure is intended to protect;
- the extent to which the challenged measure contributes to the realisation of the end pursued by that measure; and
- the trade impact of the challenged measure.[129]

Subsequently, a process of 'weighing and balancing' is used when comparing the challenged measures with 'reasonably available' WTO-consistent alternatives and their relationship to the interest pursued.[130] Only existing *measures,* and not *measures* that include a process of consultation, will be considered as 'reasonably available' alternative *measures.*[131]

Importantly, it is left to the EU, as the party maintaining the alleged WTO-inconsistent measure, to demonstrate that its Article 25(1) *measure* is necessary in light of the above.

## 5.3 Applying the 'two-tier test'

### 5.3.1 Exception at Article XIV c) ii)

The exception at Article XIV c) ii) of the *Gats* gives WTO Members, such as the EU, regulatory autonomy with respect to *measures* taken in privacy protection that are necessary

[128] *US-Gambling* (n 119) para.292
[129] Appellate Body Report *Korea- measures affecting imports of fresh, chilled and frozen beef (various measures on beef*) WT/DS161/AB/R &WT/DS169/AB/R adopted on 11 December 2000, paras.162 & 163-166
[130] *US-Gambling (*n 119*)* para.305 ff. while making reference to *Korea-various measures on beef* (n 134)
[131] *US-Gambling* (n 119) para.326

to secure compliance with laws and regulations. However, *measures* taken under such an exception are to be construed narrowly.[132]

*Is Article 25(1) a related interest?*

The first requirement to be satisfied is whether the (privacy protection) interest protected by the (adequacy requirement) *measure* relates to the privacy interest protected by the Article XIV c) ii) exception. Prima facie, Article 25(1) of the *Directive* satisfies the nexus requirement, as supported by the full text of the *Directive*. There is nothing to refute the fact that there is a 'degree of connection' between the *measure* taken at Article 25(1) of the *Directive* and the interest of privacy protection.

*Satisfying the Necessity requirement*

An analysis of the 'necessity' of the *measure* must now be undertaken in light of the steps provided in Section 5.2 of this thesis. The standard of necessity applied is accepted as being an objective standard.[133] Referencing the 'necessary' requirement, the Appellate Body in *Korea- vario*us *measures on beef*[134] case found that: '[…]Those measures which are indispensable or of absolute necessity or inevitable to secure compliance certainly fulfil the requirements…But others may fall within the ambit of that exception.'

*Does Article 25(1) protect an important interest or value, and does the Article contribute to the end pursued?*

The privacy of EU data subjects, and the value afforded to the right of privacy, requires consideration under this step. The EU would likely submit that the adequacy requirement is a means by which a high level of privacy protection is upheld, and that it ensures that the

[132] WTO S/L/74 (1999) para.14
[133] *US-Gambling* (n 119) para.304
[134] (n 129) para.157

objectives of the *Directive* per se are met. The EU regards data protection as a fundamental right and accordingly, it is protected by the EU Constitution (discussed at Chapter 2.2 of this thesis). However, varying approaches and the weight given to the right to information privacy around the world confuses the situation.

It is difficult to assess the weight that a WTO Panel and Appellate Body would give to the protection of privacy; namely, whether it would be considered important enough by the adjudicatory arms of the WTO to meet the required standard of 'necessity'. Due to the inclusion of the privacy protection under the Article XIV exceptions, it is likely to be considered a prominent public policy objective. However, the inclusion of the term 'adequate' at Article 25(1) of the *Directive* may not be considered the only way of achieving effective privacy protection (even if it is the view held by the EU). In other words, the Panel and Appellate Body may consider that the objective of achieving a high level of privacy protection could be met by requiring a less restrictive (more universally compatible) approach than that taken under Article 25(1) of the *Directive*, and one that would not require complicated adequacy assessment processes to be undertaken in order to achieve a desired level of privacy protection.

Furthermore, justification for a *measure* can only be gleaned from the domestic laws and regulations of a Member.[135] This means that the EU can proffer only the *Directive* and related domestic instruments and official publications, such as the A29WP Opinions, to support the 'necessity' of the adequacy requirement. However, neither the WTO Panel or the Appellate Body in US-*Gambling* ruled directly on the legitimacy of regulatory objectives; rather, they pointed to cultural differences between WTO Members in policy choices. In fact, it is observed that they displayed significant sensitivity to domestic regulatory concerns.[136] To that end, the Appellate Body in US-*Gambling* was not exceedingly restrictive when assessing whether the US policies are compatible with the 'necessity test' under Article XIV c) of the *Gats*. A non-restrictive approach would support the EU's imposition of the adequacy

[135] Appellate Body Report *Mexico – Tax measures on soft drinks and other beverages* WT/DS308/AB/R adopted on 6 March 2006, para 69
[136] Wunsch-Vincent (2006) p.348

requirement as a 'necessary' *measure* because of the EU's perceived 'value' that the interest of privacy is fundamental.

However, this analysis is based on the only available case on the Article XIV exceptions. Thus, a distinction may be drawn between the public moral and public order exception relied upon in US-*Gambling*, and the privacy protection exception relied upon here. US-*Gambling*, as the case name implies, dealt with restrictive gambling *measures* that were found to protect public morals and public order because they serve societal interests that can be characterized as 'vital and important in the highest degree'.[137] The EU may face a hurdle in arguing that the adequacy requirement is necessary for the same reasons; that is, that without it, there may be adverse effects on the fabric of society, similar to those caused by gambling addiction. This is only if a Panel and Appellate Body do not afford the EU the same 'sensitivity to domestic regulatory concerns' afforded to the US in *US-Gambling*.

Overall, it is difficult to say whether a Panel or Appellate Body would determine that the adequacy requirement at Article 25(1) of the *Directive* is of sufficient 'necessity' for securing compliance with laws or regulations. There is however a good chance that the EU will convince a Panel or Appellate Body that the adequacy requirement meets the 'necessity test'.

*Does Article 25(1) impact on trade?*

The restrictive impact of Article 25(1) of the *Directive* on international commerce can also be considered.[138] Article 25(1) mandates a restriction on the transfer of personal data to third countries that are found not to offer an 'adequate' level of protection. However, the *contract derogation* permitted by the *Directive* reduces the restrictive nature of Article 25(1), which cannot be read in isolation from the *contract derogation*. Thus, the EU will likely establish that the adequacy requirement is not as restrictive in practice as it is suggested by

[137] *US-Gambling* (n 119) para.299
[138] *Korea- Various measures on Beef* (n 129) para.164

the wording of Article 25 (1) of the *Directive*. Attempting to prove otherwise would be problematic.

*Weighing and balancing*

In *Korea-Vario*us *Measures on Beef*[139], the Appellate Body stated that:

> It is on the basis of this 'weighing and balancing' and comparison of measures, taking into account the interests or values at stake, that a Panel determines whether a measure is 'necessary', or alternatively, whether a WTO-consistent measure is 'reasonably available'.

The process of 'weighing and balancing' involves an assessment of the 'relative importance'[140] of interests or values furthered by the challenged *measure,* Article 25(1) of the *Directive,* and the 'reasonable availability' of an alternative measure.

The relative importance of the adequacy requirement can be established by reviewing the EU's characterisation of the objectives, and of the effectiveness of the regulatory approach of Article 25(1) of the *Directive.* Evidence of this may be found in the *Directive,* its history, and other related pronouncements.[141] As previously discussed, the *Directive* is heralded as providing the highest level of privacy protection in the world. This is supported by the *Directive* per se, and the European regard (generally) to protecting information privacy as a fundamental right.

[139] (n 129) para.166
[140] *US- Gambling* (n 119) para.102. See also: WTO Appellate Body Report *EC- measures affecting asbestos and asbestos-containing products (EC-asbestos)* WT/DS135/AB/R adopted on 12 March 2001, para.172
[141] (n 135)

However, guidance may also be found in the structure and the operation of the *measure,* and in contrary evidence proffered by the complaining party.[142] The fact that trade considerations were a supreme consideration in the adequacy findings of the US *SHA* and the *NZ Act* means that this can be 'weighed and balanced' against the relative importance of the adequacy requirement, and can also undermine the 'necessity' of the adequacy requirement. The adequacy criterion was overlooked in favour of the economic interests of the EU when finding adequacy in the US *SHA* and the *NZ Act* respectively.

Thus, the EU's message is clear: that the adequacy requirement is only necessary to the extent that it does not hinder trade relations, and conversely, adequacy is less necessary where there is limited trade at issue. On that basis, the EU will face a hurdle in establishing the importance of the adequacy requirement, and in establishing that there is no 'reasonably available' alternative.

A 'reasonably available' *measure* is, arguably found in the *contract derogation* or in the form of an agreement similar to the US *SHA*. The *contract derogation* is supported by the standard model contractual clauses drafted by the EU. These standard contractual clauses may be found to constitute a 'reasonably available' measure, and to reduce the need for the adequacy requirement in its current form, which requires an assessment of third country privacy protection systems that has resulted in an inconsistent application of the inconclusive adequacy criterion. The *contract derogation* may represent '[…]A measure that would preserve for the responding member its right to achieve its desired level of protection with respect to the objective pursued.'[143] The EU would, in response, have to point out why the *contract derogation* would not achieve the same objectives as the adequacy requirement under Article 25(1) of the *Directive.*[144] It is unlikely that the EU would be able to do so, especially in light of the Commission and A29WP having strayed from the adequacy requirement in delivering the (trade-based) findings that adequacy existed in the US *SHA* and the *NZ Act.* Such decisions ultimately undo the necessity of the adequacy requirement.

[142] *US-Gambling* (n 119) Para.304 citing Appellate Body Report *India - Patent Protection for Pharmaceutical and Agricultural Chemical Products* WT/DS50/AB/R adopted on 19 December 1997, para.66
[143] *EC-Asbestos* (n 140) paras.172-174
[144] Required in light of the judgment in *US-Gambling* (n 119) paras.309-310

In any event, the EU must prove that it meets the requirements of the *Chapeau* to Article XIV of the *Gats* before it can be determined whether the adequacy requirement is a WTO-consistent *measure*.

### *5.3.2 Chapeau* to Article XIV

A *measure* under the *Chapeau* may be analysed regardless of whether the *measure* is, or is not, provisionally justified under subsection c) ii) of Article XIV of the *Gats*. Of the standard requirements at the *Chapeau*, Article 25(1) of the *Directive* must not be found to constitute arbitrary or unjustifiable discrimination between countries where the same conditions prevail.

This section seeks to show that the inconsistency of the application of the adequacy requirement to the US *SHA*, the *NZ Act*, and the *Australian Act* could present the prohibited 'arbitrary or unjustifiable discrimination'.

The idea of making non-discrimination the focus of the *Gats* commitments recently surfaced in the context of WTO negotiations.[145] In US-*Gambling*[146], the Appellate Body stated that the focus of the *Chapeau* serves to ensure that Members' rights to avail themselves of exceptions if they exercise the exceptions reasonably, so as not to frustrate the rights accorded to other Members by the substantive rule of non-discrimination of the *Gats*.

In US-*Gambling*, both the Panel and the Appellate Body confirmed that discrimination of some sort was anchored in the US *measures*, or practised through selective enforcement.[147] The idea of selective enforcement is relevant to the the EU's selective accommodation of trade considerations in deciding upon the adequacy of the US *SHA* and the *NZ Act*, and when enforcing the adequacy requirement strictly on the *Australian Act*, and with no regard for trade considerations. Thus, Australia could make prima facie case of discrimination against the EU.

[145] Wunsch-Vincent (2005) p.347
[146] *US-Gambling* (n 119) para.339
[147] *US-Gambling* (n 119) paras. 364-366. Although, these were initially considered in light of the full national treatment obligation under Article XVII of the *Gats*.

However, the Appellate Body in US-*Gambling* was not exceedingly restrictive when assessing whether the US policies were compatible with the requirement of non-discrimination under the *Chapeau*, save for legislation that permitted domestic, but not foreign, service suppliers to offer remote betting services on horseracing. That legislation supported the contention that discrimination between domestic and foreign service providers did not satisfy the requirements of the *Chapeau.*[148] It may be relevant here that the EU Member States have been found to inconsistently transcribe the *Directive* into national laws, and this has resulted in breaches of the *Directive*. Despite this, the EU imposed the adequacy requirement strictly on the *Australian Act.*

In addition, the requirement of the *Chapeau* relating to 'where like conditions prevail' must also be satisfied. Precisely what the WTO adjudicatory arms would consider as constituting 'like conditions' is unknown. The EU may contend that 'like conditions' do not prevail between Australia, the US and New Zealand. It would claim that the trade power (the focus of the adequacy ratings afforded to the US *SHA* and the *NZ Act*) of Australia was not as substantial as the trade power of the US and, thus, did not reflect a situation where 'like conditions prevail'. Similarly, the EU could argue that the geographic and economic isolation of New Zealand differs from Australia's situation. Obviously, the geographical isolation argument is easily refutable; however, New Zealand's economic situation is vastly different to Australia's, largely due to the smaller size and resources of the former. However, the provision for 'like' conditions as opposed to, for example, 'identical' conditions may be construed as sufficiently flexible to favour Australia's claim, and to support the contention that the EU applied its adequacy requirement in a discriminatory manner to third countries 'where like conditions prevail'.

Overall, it is more likely that the EU will face difficulties persuading a Panel or Appellate Body that it did not apply the adequacy requirement in an arbitrary or unjustifiable discriminatory manner to the *Australian Act*. The *Australian* Act was subjected to a rigid application of the adequacy criterion; this differed from the EU's treatment of the US *SHA* and the *NZ Act.* This aspect of the *Chapeau* is relevant regardless of whether Article 25(1) is found to be provisionally justified under the Article XIV c) ii) exception.

[148] *US-Gambling* (n 119) para. 368-369

## 5.4 Summary of likely findings: Australia v the EU

The EU would undoubtedly rely on the general privacy protection exception at Article XIV c) ii) of the *Gats* to preserve the inconsistent bases for its adequacy findings. However, whether the EU can prove the 'necessity' of the adequacy requirement is uncertain, in light of: the *contract derogation;* and the uncertain degree of importance the WTO adjudicatory arms place on the right to information privacy, while having regard to the differing approaches taken around the world. Previous Panel and the Appellate Body reluctance to determine the legitimacy of a Member's regulatory objectives would likely favour the EU's case.

Although the adjudicatory arms of the WTO have provided little guidance as to what constitutes a 'discriminatory' measure, US-*Gambling* shows that policy-based exceptions are permitted flexibility. The *measure* at Article 25(1) of the *Directive,* which has arguably been applied more strictly to the letter of the *Australian Act* and without any consideration for trade – in contrast to the EU's treatment of the US *SHA* and the *NZ Act* – could be found to be discriminatory and, thus, WTO-inconsistent.

Should the EU wish to rely upon the general exception for privacy in the future pursuant to Article XIV c) ii) of the *Gats*, this could, in turn, support a new WTO precedent that the adequacy requirement and the supporting criterion should be applied on the same terms for all third countries or, at least, all third countries 'where like conditions prevail'.

For completeness, if it were the case that Article 25(1) of the *Directive* is a *measure* which does not satisfy all the requirements of an Article XIV c) ii) exception, then Article 25(1) would be required to meet all other *Gats* obligations. The applicability of the obligations would be viewed in light of the EU's schedule of Commitments and any listed Most-Favoured Nation Treatment exemptions. The scope of this thesis does not extend to that analysis.

## 5.5 Conclusion: the EU v Australia

WTO Members wishing to impose privacy protection measures on other WTO Members appear to have fairly straightforward access to qualifying for an Article XIV c) ii) *Gats* exception. In principle, findings under Article XIV are permitted so long as the pursued policy objectives represent a listed interest. The effect of the exception is that WTO Members are entitled to contravene their other obligations under the *Gats*. However, they are also subject to the requirement that *measures* are not applied in a manner which would constitute a means of 'arbitrary or unjustifiable discrimination between countries where like conditions prevail'.

It is likely that Article 25(1) of the *Directive* would be found to fall within the privacy protection exception at Article XIV c) ii) of the *Gats*. However, the EU would not necessarily be able to prove that the Article 25(1) requirement of adequacy was applied consistently to third countries in line with the *Chapeau* at Article XIV of the *Gats*.

# 6 Conclusion

## 6.1 Overview

The main objective of this thesis is to address the adequacy requirement at article 25(1) of the *Directive*, together with the inconsistent application of what is an inconclusive adequacy criterion.

This thesis also seeks to shed light upon the way in which the Commission and the A29WP applied the adequacy criterion strictly to the *Australian Act* and consequently, found that the level of protection offered by that Act was not 'adequate' for the purpose of Article 25(1) of the *Directive*. In contrast, a more lenient and trade-based approach was taken in the assessment of the US *SHA* and the *NZ Act*. This resulted in findings of adequacy.

This thesis also examines the possible implications of the inconsistent application, and selective expansion of the adequacy criterion to include trade considerations, in light of Article XIV of the *Gats*.

## 6.2 The EU approach to protecting personal information privacy in transborder data transfer

The strength of the wording of Article 25(1) reflects the European approach to protecting information privacy as a fundamental right. It also suggests that that the Commission demands to be taken seriously when it purports to prevent transborder transfers of the personal data of its citizens. However, the opposite effect is had when, despite A29WP attempts to define the adequacy requirement, that concept remains inconclusive. The bite of the adequacy requirement is further weakened by the Commission and the A29WP's selective alteration of the criterion to include trade considerations upon which they may make adequacy findings.

## 6.3 The 'non-adequate' Australian approach to protecting personal information privacy in transborder data transfers

The A29WP concluded that a number of aspects of the *Australian Act* amounted to deficiencies in the level of privacy protection offered by the *Australian Act.* However, this was arguably the result of a strict application of the adequacy criterion to the *Australian Act.*

An examination of the issues of contention between Australia and the EU, also highlight the extent to which differing approaches to legislating for information privacy protection complicate the adequacy assessment process. The adequacy requirement would better achieve the high level of information privacy protection it mandates if there existed a universally accepted level to which the right to privacy is respected, namely that data protection privacy is a fundamental right. They can also lead to a misunderstanding of aspects of a third country's privacy protection system. This occurred during the A29WP's assessment of the adequacy

The fact that the *Australian Act* is currently undergoing a major overhaul – including reform to the SB and ER Exemptions and NPP9 – may assist in the *Australian Act* attaining an adequacy rating from the EU. However, the fact that the adequacy criterion remains inconclusive and susceptible to selective alteration means that forecasting adequacy ratings for any third country is wrought with unpredictability.

## 6.4 Assessments of other third country personal information privacy protection systems

The application of the adequacy criterion to the *Australian* Act, as compared to its application to the US *SHA* reflects at best an inconsistent application, and at worst, a discriminatory application.

In that regard, neither the US *SHA* nor the *Australian Act* met the letter or the intent of the *Directive*. However, the former received an adequacy rating based on its trade relationship with the EU; Australia, on the other hand, did not attain such a rating as it did not have a

sufficient trade relationship to do so. Additionally, it has been shown that the *NZ Act* produced some deficiencies on assessment, but still received an adequacy rating; this is because its relatively small trade exposure was considered too insignificant to pose an information safety threat.

## 6.5 Implications of the inconsistent application of the adequacy criterion

The *measure* at Article 25(1) of the *Directive*, which has arguably been applied more strictly to the letter of the *Australian Act* and without any consideration for trade – in contrast to the EU's treatment of the US *SHA* and the *NZ Act* – could be found to be discriminatory and, thus, WTO-inconsistent.

Should the EU wish to rely upon the general exception for privacy pursuant to Article XIV c) ii) of the *Gats*, this could, in turn, support a new WTO precedent that the adequacy requirement and the supporting criterion should be applied on the same terms for all third countries or, at least, all third countries 'where like conditions prevail'.

## 6.6 Final remarks

Overall, a comparative analysis of the Commission and the A29WP's treatment of the information privacy protection systems of Australia, the US and New Zealand finds that the mandated requirement for adequacy under Article 25(1) of the *Directive* is problematic. The Commission and the A29WP's inability to conclusively articulate what constitutes adequacy, the subsequent inconsistent application of the adequacy criterion to third countries, and its selective interpretation to include trade considerations, undermines the level of protection Article 25(1) purports to offer to the personal data of EU citizens, when that data is the subject of transborder transfers.

The adequacy requirement is not only selectively flexible, but its inconsistent application could constitute unjustifiable discrimination.

# 7 Reference Table

## Legislation

### EU instruments

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* [1995] OJ L281/31

Council of Europe Convention of 28 January 1981 *for the protection of individuals with regard to automatic processing of personal data* [1981] ETS 108

The European Commission *Charter of Fundamental Rights of the European Union* [2000] Official Journal C83/392

European Parliament and European Council Proposal of 25 January 2012 for a *Regulation on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation)* [2012] 2012/0011 (COD)

The European Union Treaty of 9 May 2008 (incorporating Libson Treaty Amendments) *on the Functioning of the European Union Official Journal* [2008] C 115/47

### Australian instruments

*The Privacy Act 1988* Australia (Cth) (as amended) available: http://www.comlaw.gov.au/Details/C2013C00125

Privacy Amendment (Enhancing Privacy Protection) Bill 2012 available: http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbillsdgs%2F1923143%22

An Act to Constitute the Commonwealth of Australia 1900 available: http://www.aph.gov.au/About_Parliament/Senate/Powers_practice_n_procedures/~/media/1A31A695333A450AA8A5641B6969AE12.ashx

Privacy Amendment (Private Sector) Act 2000 (Cth) available: http://www.comlaw.gov.au/Details/C2004A00748

Health Records (Privacy and Access) Act 1997 (ACT) available: http://www.legislation.act.gov.au/a/1997-125/current/pdf/1997-125.pdf

The Privacy and Personal Information Act 1998 (New South Wales) available: http://www.austlii.edu.au/au/legis/nsw/consol_act/papipa1998464/

Health Records and Information Privacy Act 2002 (New South Wales) available: http://www.legislation.nsw.gov.au/fullhtml/inforce/act+71+2002+FIRST+0+N

The Information Act 2002 (the Northern Territory) available: http://www.austlii.edu.au/au/legis/nt/consol_act/ia144/

The Personal Information Protection Act 2004 (Tasmania) available: http://www.austlii.edu.au/au/legis/tas/consol_act/pipa2004361/

The Information Privacy Act 2000 (Victoria) available: http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/4BE13AE4A4C3973ECA256E5B00213F50/$FILE/00-098a.pdf

Health Records Act 2001(Vic) available: http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/E57A0A1DDCD389FBCA256E5B00213F4D/$FILE/01-002a.pdf

The Information Privacy Bill 2007 (Western Australia) available: http://www.parliament.wa.gov.au/Parliament/bills.nsf/B76E4F86BE5ACCADC82572AB002D2C7F/$File/Bill%2B193-1.pdf

**New Zealand instruments**

New Zealand Official Information Act 1982 available*:* *http://www.legislation.govt.nz/act/public/1982/0156/latest/DLM64785.html*

New Zealand Local Government Official Information and Meetings Act 1987 available*:* *http://www.legislation.govt.nz/act/public/1987/0174/latest/DLM122242.html*

New Zealand Electoral Act 1993 available*:* *http://www.legislation.govt.nz/act/public/1987/0174/latest/DLM122242.html*

**Other instruments**

The United Nations Universal Declaration of Human Rights 1948 available at: http://www.un.org/en/documents/udhr/

The United Nations International Covenant on Civil and Political Rights 1966 available at: http://treaties.un.org/doc/Publication/UNTS/Volume%20999/volume-999-I-14668-English.pdf

*General Agreement on Tariffs and Trade* 1994, Apr. 15, 1994, Marrakesh Agreement Establishing the World Trade Organization, Annex 1A, The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 17 (1999), 1867 U.N.T.S. 187, 33 I.L.M. 1153 (1994) [hereinafter GATT 1994]

*General Agreement on Trade in Services 1994*, April 15, 1994, Marrakesh Agreement Establishing the World Trade Organisation, Annex 1B. The Legal Texts: The Results of the Uruguay Round of Multilateral Trade Negotiations 284 (1999), 1869 U.N.T.S. 183, 33 I.L.M. 1167

## Legal Cases

### ECJ

Bodil Lindqvist Case C-101\01 [2003] ECR I-12971

Rechnungshof v Österreichischer Rundfunk and Others (C-465/00, C-138/01, and C-139/01) [2003] ECR I-4989

### WTO

WTO Panel Report *China-measures affecting trading rights and distribution services for certain publications and audiovisual entertainment products,* WT/DS363/R adopted on 12 August 2009

WTO Appellate Body Report *Mexico – Tax measures on soft drinks and other beverages* WT/DS308/AB/R adopted on 6 March 2006

WTO Appellate Body Report *US-Measures Affecting the Cross-Border Supply of Gambling and Betting Services,* WT/DS285/AB/R adopted on 7 April 2005

WTO Appellate Body Report *Mexico- measures affecting telecommunications services* WT/DS204/R adopted on 2 April 2004

WTO Appellate Body Report *EC- Measures Affecting Asbestos and Asbestos-Containing Products* adopted on 12 March 2001(WT/DS135/AB/R)

WTO Appellate Body Report *Korea- Measures Affecting Imports of Fresh, Chilled and Frozen Beef* adopted on 11 December 2000 (WT/DS161/AB/R, WT/DS169/AB/R)

WTO Appellate Body Report *India - Patent Protection for Pharmaceutical and Agricultural Chemical Products* adopted on 19 December 1997 *(* WT/DS50/AB/R)

## Official publications

### Article 29 Working Party Documents

Article 29 Working Party *Discussion Document: First Orientations on Transfers of Personal Data to Third Countries - Possible Ways Forward in Assessing Adequacy* adopted on 26 June 1997 (WP 4)

Article 29 Working Party *Working Document: Transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive* adopted on 24 July 1998 (WP 12)

Article 29 Working Party *Working Document: Judging Industry Self- Regulation: When does it make a meaningful contribution to the level of data protection in a third country?* adopted on 14 January 1998 (WP7)

Article 29 Working Party *Opinion 7/99 on the level of data protection provided by the "Safe Harbor" Principles as published together with the Frequently Asked Questions (FAQs) and other related documents* on 15 and 16 November 1999 *by the* US *Department of Commerce* adopted on 3 December 1999 (WP 27)

Article 29 Data Protection Working Party *Opinion 3/2001 on the level of protection of the Australian Privacy Amendment (Private Sector) Act 2000* adopted on 26 January 2001 (WP40)

Article 29 Working Party *Opinion 4/*2002 *on the level of protection of personal data in Argentina* adopted on 3 October 2002 (WP 63)

Article 29 Working Party *Opinion 5/2003 on the level of protection of personal data in Guernsey* adopted on 13 June 2003 (WP79)

Article 29 Working Party *Document Transfers of personal data to third countries: Applying Article 26 (2) of the EU Data Protection Directive to Binding Corporate Rules for International Data Transfers* adopted on June 3 2003 (WP 74)

Article 29 Working Party *Working document on a common interpretation of Article 26(1) of Directive 95/46/EC* adopted on 25 November 2005 (WP114)

Article 29 Working Party *Opinion 6/2009 on the level of protection of personal data in Israel* adopted on 1 December 2009 (WP 165)

Article 29 Working Party, together with the Working Party on Police and Justice on *The Future of Privacy – Joint Contribution to the Consultation of the European Commission on the Legal Framework for the Fundamental Right to Protection of Personal Data* adopted on 1 December 2009 (WP168)

Article 29 Working Party *Working Document on Frequently Asked Questions (FAQs) related to Binding Corporate Rules* revised and adopted on 8 April 2009 (WP155 rev 04)

Article 29 Working Party *Opinion 6/2010 on the level of protection of personal data in the Eastern Republic of Uruquay* adopted on 12 October 2010 (WP177)

Article 29 Data Protection Working Party *Opinion 11\2011 on the level of protection of personal data in New Zealand* adopted on 4 April 2011 (WP 182)

**European Commission Publications**

Commission Decision 2000/520/EC pursuant to Directive 95/46/EC of the European Parliament and of the Council *on the adequacy of the protection provided by the safe harbour privacy principles and related frequently asked questions issued by the US Department of Commerce* on 26 July 2000 [OJ L 215, 25/8/2000]

Commission First Report *on the implementation of the Data Protection Directive (95/46/EC)* of 15 May 2003 [COM/2003/265] available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:52003DC0265:EN:NOT

### Australian Government Publications

The Parliament of the Commonwealth of Australia, House of Representatives. *Privacy Amendment (Enhancing Privacy Protection) Bill 2012 Explanatory Memorandum* (2012) http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728/upload_pdf/368711.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r4813_ems_00948d06-092b-447e-9191-5706fdfa0728%22

*Australian* Law Reform Commission. *Privacy.* Report No 22 (1983) http://www.austlii.edu.au/au/other/alrc/publications/reports/22/

*Australian* Law Reform Commission. *For Your Information: Australian Privacy Law and Practice Report No 108* (2008). Volumes 1 – 3 http://www.alrc.gov.au/publications/report-108

Honorable Daryl Williams AM QC MP, Attorney-General. *Second Reading Speech to the Privacy Amendment (Private Sector) Bill 2000* to the House of Representatives on 12 April 2000 (Hansard 12.4.2000)

### WTO documents

WTO Council of Trade in Services. *Trade in Services: Work Programme on Electronic Services: Progress Report to the General Council* adopted on 19 July 1999 (S/L/74)

WTO Council for Trade in Services. *Guidelines for the Scheduling of Specific Commitments under the General Agreement on Trade in Services* adopted on 23 March 2001 (S/L/92)

### Data Protection Privacy Agreements

Agreement between the European Union and Australia *on the processing and transfer of Passenger Name Record (PNR) data by air carriers to the Australian Customs and Border Protection Service of 29 September 2011* adopted on 14 July 2012 [OJL 186/4]

## Secondary Literatures

### Books

Heisenberg Dorothee, *Negotiating Privacy: The European Union, the United States and Personal Data Protection.* London, (Lynne Reinner Publishers) 2005

Kuner Christopher, *European Data Protection Law: Corporate Compliance and Regulation* (2nd ED.) New York, (Oxford University Press) 2007

D Solove, M Rotenberg and P Schwartz, *Information Privacy Law* (2nd ed.) New York, (Aspen Publishers) 2006

### Articles

Bygrave Lee. *Privacy and Data Protection in an International Perspective.* In: Scandinavian Studies in Law. Volume 56 (2010)

Bygrave Lee and G Greenleaf. *Not Entirely Adequate but Far Away: Lessons from how Europe Sees New Zealand Data Protection*. In: Privacy Laws & Business International Report, Issue 111 (2011)

Dan Jerker and B. Svantesson. *Privacy, the Internet and Transborder Data Flows – An Australian Perspective.* In: Masaryk University Journal of Law and Technology. Volume 4.1 (2010)

Esayas, Samson Yoseph. *A Walk in to the Cloud and Cloudy It Remains: The Challenges and Prospects of 'Processing' and 'Transferring' Personal Data.*In: Computer Law & Security Review. Volume 28 (2012)

Ewing, M. *The Perfect Storm: The Safe Harbor and the Directive on Data Protection.* In: Houston Journal of International Law. 315 (2002)

Ford, Peter. *Implementing the EC Directive on Data Protection – an outside perspective.* In: Privacy Law and Policy Reporter. Volume 9 (2003)

Greenleaf, Graham and Nigel Waters. *Australia's Privacy Bill 2012: Weaker Principles, Stronger Enforcement*. In: Privacy Laws and Business International Report. Issue 118 (2012)

Greenleaf, Graham. *The Influence of European data privacy standards outside Europe: implications for globalization of Convention 108.* In: International Data Privacy Law Online. Volume 2(2) (2012)

Greenleaf, G and Lee Bygrave. *Not Entirely Adequate but Far Away: Lessons from how Europe Sees New Zealand Data Protection*. In: Privacy Laws & Business International Report, Issue 111 (2011)

Lindsay, David. *An Exploration of the Conceptual Basis of Privacy and the Implications for the Future of Australian Privacy Law.* In: Melbourne University Law Review. Volume 29 (2005).

Mattli, W and T Buthe. *Setting International Standards: Technological Rationality or Primacy of Power?* In: World Politics. Volume 56, No. 1 (2003)

Newman, Abraham L. *Building Transnational Civil Liberties: Trans governmental Entrepreneurs and the European Data Privacy Directive*. In: International Organization. Volume 62, No. 1 ( 2008)

Pauwelyn, Joost. *WTO Softens Earlier Condemnation of U.S. Ban on Internet Gambling, but Confirms Broad Reach into Sensitive Domestic Regulation*. In: American Society of International Law Online. (2005)

Shaffer, Gregory. *Globalisation and Social Protection: The Impact of EU and International Rules in the Ratcheting Up of U.S. Data Privacy Standards.* In: Yale Journal of International Law. Volume 25 (2000)

Shin-yi Peng. *Comments on the U.S.-Antigua Internet Gambling Dispute: Contextual Interpretation and Framework of Market Access and National Treatment.* In: Chengchi Law Review. Volume 85 (2005)

Sylvia Kierkegaard, Nigel Waters, Graham Greenleaf, Lee A. Bygrave. Ian Lloyd, Steve Saxby. *30 Years On – The Review of the Council of Europe Data Protection Convention 108*. In: Computer Law and Security Review. Volume 27 (2011)

Tan, J. *A Comparative Study of the APEC Privacy Framework – a New Voice in the Data Protection Dialogue?* In: Asian Journal of Comparative Law. Volume 3, Issue 1 (2008)

Waters, Nigel. *The European Influence on Privacy Law and Practice.* In: Privacy Law and Policy Reporter. Volume 9 (2003) http://www3.worldlii.org/au/journals/PLPR/2003/2.html accessed 15 January 2013

Waters, Nigel. *Privacy Impact Assessment in Hong Kong from an International Perspective*. In: University of New South Wales Faculty of Law Research Series (2010)

Waters, Nigel and Greenleaf Graham. *A Critique of AUStralia's Proposed Privacy Amendment (Enhancing Privacy Protection) Bill 2012*. In: University of New South Wales Law Review. Volume 35 (2012)

Weber, Rolf H. *Digital Trade in WTO Law - Taking Stock and Looking Ahead.* In: Asian Journal of WTO & International Health Law and Policy. Vol. 5, No. 1 (2010) http://dx.doi.org/10.2139/ssrn.1578139 accessed 29 April 2013

Weber, Rolf H. *Regulatory Autonomy and Privacy Standards Under the the GATS*. In: Asian Journal of WTO & International Health Law and Policy. Volume 7, No. 1 (2012) http://ssrn.com/abstract=2117854

Wunsch-Vincent, Sacha. *The Internet, Cross- Border Trade in Sevices, and the GATS: Lessons from* US-*Gambling.* In: World Trade Review. Volume 5:3 (2006)

## Conference Papers

Coper, Michael. *Three Good Things and Three Not-so-Good Things About the Australian Legal System* (International Association of Law Schools Conference: Learning from Each Other: Enriching the Law School Curriculum in an Interrelated World, China, 17-19 October 2007) http://www.ialsnet.org/meetings/enriching/coper.pdf

Greenleaf, Graham. *Exporting and Importing Personal Data: the effects of the Privacy Amendment (Private Sector) Bill 2000* (National Privacy and Data Protection Summit, IBC Conferences, Sydney, 17 & 18 May 2000)

Waters, Nigel. *The APEC Asia-Pacific Privacy Initiative – a new route to effective data protection or a trojan horse for self-regulation?* (Privacy Laws and Business 21st Annual International Conference, Cambridge, 8 July 2008)

## Submissions

Greenleaf, Waters, N and Lee Byrgave. *Implementing privacy principles: After 20 years, it's time to enforce the Privacy Act* (submission to the *Australian* Law Reform Commission on the Review of Privacy Issues Paper, Cyberspace Law and Policy Centre. 31 January 2007

Greenleaf, Graham. *Comparative Study: Different Approaches to New Privacy Challenges In particular In Light of Technological Developments*: *Country Studies B.2 – AUStralia* (submission to the European Commission Directorate – General Justice, Freedom and Security) (2010) [ JLS/2008/C4/011 – 30-CE-0219363/00-28]

Waters, Nigel and Greenleaf, Graham for the *Australian* Privacy Foundation *on the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 by the Australian Privacy Foundation* (submission to the *Australian* Senate Legal and Constitutional Affairs Legislation Committee, and to the House of Representatives Standing Committee on Social Policy and Legal Affairs) (2012)

**Press Release**

Office of the New Zealand Privacy Commissioner. *European Union endorses New Zealand Privacy Act*, 20 December 2012. Online media release available at www.privacy.org.nz/EUropean-union-endorses-new-zealand-privacy-act-media-release