Canadian Journal of Law and Technology

Volume 8 | Number 1 Article 1

6-1-2010

# Inadequate: The APEC Privacy Framework & Article 25 of the European Data Protection Directive

Stuart Hargreaves

# Inadequate: The APEC Privacy Framework & Article 25 of the European Data Protection Directive

*Stuart Hargreaves*[*]

## INTRODUCTION

An ever-increasing amount of personal information about the habits, actions, beliefs, and opinions of individuals is collected and stored by organisations. A new generation of computers using sophisticated algorithms can process this mass of raw data into valuable records that can be then sold for a variety of purposes. Data from retail "loyalty" cards or credit cards might be processed in order to understand an individual's consumption preferences and habits, which would be of significant interest to marketers.

> Online commercial transactions depend on both the creation and availability of unprecedented and extensive data about individuals . . . [this] pushes a dramatic increase in the importance of data privacy issues for consumers, business, and society.[1]

Data collected by telecoms, airlines, and credit card companies might be processed by a state in order to try to uncover the movements of terror cells. A broad spectrum of data might be processed to develop very detailed profiles of single individuals to target them in an electoral campaign. The value — economic or otherwise — of processed data is immense, and so creates tremendous incentives for both the state and the private sector to collect as much personal data about individuals as they can.

Naturally, there are corresponding incentives for individuals to learn just when, how, and why this data is being collected and processed. In response to public demand, some governments have pushed for data protection regimes to combat potential abuses in the collection and processing of personal information. The European Union's Data Protection Directive[2] offers comparatively high levels of control to individuals over their personal information and is backed up by strong enforcement mechanisms; the Directive represents the current high-water mark of data protection. The Asia-Pacific Economic Co-operation group (APEC) has re-

---

* B.A. (McGill), LL.B (Osgoode Hall), B.C.L. (Oxford), S.J.D. Candidate (Toronto) Barrister & Solicitor, Law Society of Upper Canada. stuart.hargreaves@utoronto.ca.

1 Joseph Reidenberg, "E-Commerce and Transatlantic Privacy" (2001) 38 Hous. L. Rev. 717 at 719.

2 EC, *Council Directive 95/46/EC of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, [1995] O.J. L 281/31 [*Directive*].

cently adopted a more business-friendly "Privacy Framework"[3]; Google has led the way in pushing this Framework as a model for a new global consensus.[4] The EU and APEC approaches represent two different ways of thinking about the purpose of privacy rights in personal information (a.k.a. "informational privacy" or "data privacy"). The European approach sees integrity and control over information about oneself as inherent to human dignity; informational privacy is treated as a fundamental right subject only to limited restrictions. In contrast, the approach evinced by APEC is a market-oriented cost/benefit calculus; control over personal information is seen as a beneficial policy goal when it can increase consumer confidence and promote economic growth — the implication being that it can also more easily give way in the face of competing economic arguments. These two approaches — one grounded in the language of rights, the other in the language of markets — result in significant differences in both the substantive and procedural protections each regime creates. This article argues that the two approaches are incompatible, and the tension this creates is revealed in the rules regarding the transfer of personal data from Europe to third countries.

Article 25 of the Directive requires the European Commission to determine that "adequate" data protection laws are in place in third states before personal data collected in the EU can be transferred outside its borders. Under Articles 29 and 30, an independent "Working Party" is created to advise the Commission on the level of data protection in third states. According to the Working Party's approach, an "adequate" data protection regime is one which meets a particular core of substantive and procedural protections. This paper suggests that if the APEC Framework were to be implemented as domestic legislation in an APEC Member economy, any such legislation would not meet this core; the Commission, therefore, should not consider any future legislation modelled on the APEC Framework to be "adequate," barring significant upgrades to its provisions. Given this apparent inadequacy, I also consider whether the American "Safe Harbor"[5] agreement with the EU could represent an alternative approach upon which negotiation between APEC and the EU could be based. However, I ultimately reject this on both practical and ideological grounds. The Commission ought instead to lobby for domestic legislation in APEC Member economies that is truly "adequate," and until those economies implement such sufficiently robust data protection regimes, rely upon individual contractual measures[6] between EU-based and APEC-based organizations to ensure the adequate protection of transmitted personal information.

---

3 APEC, *Privacy Framework* Doc. No. 205-SO-01.2 (2005), online: APEC <http://www.apec.org> [*APEC Framework*].

4 In September 2007, Google's Chief Privacy Counsel described the APEC Framework as "the most promising foundation" upon which to build a global set of privacy laws for personal information. Peter Fleisher, *The Need for Global Privacy Standards*, online: Peter Fleischer: Privacy? <http://PeterFleischer.blogspot.com/2007/09/need-for-Global-Privacy-Standards.html/>.

5 US Department of Commerce, *Issuance of Safe Harbor Principles and Transmission to the European Commission* 65 Fed. Reg. No. 142 (2000) [*Safe Harbor*].

6 *Directive*, *supra* note 2, Art. 26(2).

In support of the contention that the APEC Framework or legislation modelled upon it cannot be considered an "adequate" data protection regime, this article will first trace the competing theoretical approaches to privacy that the APEC Framework and the EU Directive represent, and will then outline the major substantive and procedural protections each regime offers. The potential adequacy of the APEC Framework will then be assessed from the perspective of the requirements outlined by the Working Party, by reflecting on both the stated policies and past recommendations it has made to the Commission regarding data protection regimes in third states.

## I. PRIVACY AND CONTROL OF PERSONAL INFORMATION

Reilly suggests that it was the process of industrialisation that led to the first Western legal recognition of privacy: the development of photography, radio, and widely read newspapers created an increased threat to an individual's privacy through public dissemination of information about his/her life.[7] Responding to these developments in the United States at the end of the 19th century, Warren and Brandeis argued that an individual should have the "right to be let alone" and the "right to one's personality."[8] More than one hundred years on, privacy, as a legal concept, has diversified and expanded in myriad ways beyond this relatively narrow view; this article does not, however, seek to define its precise contours and limits. Rather, it is premised on the idea that at least *one* aspect of privacy is the ability of individuals to have at least *some* level of control over when and how their "personal" information is recorded and processed; this we can term as "informational privacy" or "data privacy."

Fried, for example, believes that privacy "is not simply the absence of information about us in the minds of others; rather it is the *control* we have over information about ourselves" [emphasis in original].[9] Miller thinks "the basic attribute of an effective right of privacy is the individual's ability to control the circulation of information relating to him."[10] A widely-accepted variant is put forth by Westin, who argues that "privacy is the claim of individuals, groups or institutions to determine for themselves when, how and to what extent information about them is communicated to others."[11] This is perhaps the liberal claim to informational privacy *par excellence* — it locates the key element of privacy as the power of the individual to choose when and how she will distribute her personal information. Information that is properly deemed as attracting a privacy interest is generally considered beyond the reach of other individuals or the state, creating a zone of privacy that allows the individual to fully exercise her autonomy and have her dignity, as a person, respected.

---

7 Robert A. Reilly, "Conceptual Foundations of Privacy: Looking Backward before Stepping Forward" (1999) 6:2 Rich. J.L. & Tech. 6 at 7.

8 Samuel Warren & Louis Brandeis, "The Right to Privacy" (1890) 4:5 Harv. L. Rev. 193 at 215.

9 Charles Fried, "Privacy" (1967) 77 Yale L.J. 475 at 482.

10 Arthur Miller, *The Assault on Privacy* (Ann Arbor: University of Michigan Press, 1971) at 25.

11 Alan F. Westin, *Privacy and Freedom* (New York: Atheneum, 1967) at 7.

In legislative terms, this control may take the form of substantive rules regarding when and how the state, corporations, or other organisations may collect and process personal information, and associated procedural rules to ensure effective enforcement. Precisely how much control individuals should be given is, of course, a matter of strenuous debate, and that is reflected in the approaches to data privacy outlined here.

The EU approach positions data privacy as an inherent human right that can only be limited in rare situations; in contrast, the APEC approach eschews the language of rights entirely, instead treating data privacy as a policy interest aimed at ensuring continued growth in an increasingly internet-based economy. These are fundamentally different normative approaches: are privacy rules simply part of a broader economic policy designed to promote growth, or do they exist to guarantee a human right that helps to promote individuality, dignity, and autonomy? The APEC Framework takes the former approach, positioning privacy in personal information as a policy that is relatively easily balanced against competing economic interests. It treats a (limited) level of control over one's own personal information as an instrumental good that can remedy imbalances in the "information marketplace," since in the absence of appropriate regulation it is argued that:

> [T]he company . . . does not suffer losses from the disclosure of private information. Because customers often will not learn of the overdisclosure, they may not be able to discipline the company effectively. In economic terms, the company internalizes the gains from using the information but can externalize some of the losses and so has a systematic incentive to overuse it.[12]

On this account, data privacy rules can perform a regulatory function that forces business to take better account of the interest consumers have in their personal information. Those who see privacy as essentially a regulatory tool are fearful of the costs that a more robust form of legislated privacy might impose on business. For example, Walker argues that higher regulatory burdens threaten to chill the creation of innovative goods and services and even alter social values, making privacy "burdensome for individuals and a dicey proposition for society at large."[13] Individuals will pay more as a result of an increased regulatory burden on corporations, less choice, and have less opportunity to receive tailored services. Walker feels that even tailored *advertising* is ultimately to the benefit of consumers because they are more likely to receive advertisements of interest to them, and because it reduces the marketing costs of business, with the savings passed on to consumers.[14] The APEC Framework reflects similar thinking, treating informational privacy as valuable only to the extent that it can increase consumer confidence. Its provisions belie a normative approach that sees data privacy rules as having the potential to stimulate growth, but if the rules created are too robust, they risk having the opposite effect by being burdensome on business. The extent of

---

12 Peter P. Swire & Robert E. Litan, *None of Your Business: World Data Flows, Electronic Commerce, and the European Privacy Directive* (Washington, DC: Brookings Institution Press, 1998) at 8.

13 Kent Walker, "The Costs of Privacy" (2001) 25 Harv. J.L. & Pub. Pol'y 87 at 88.

14 Ibid. at 90.

control over personal information granted to individuals is, therefore, always to be balanced between these two concerns. Beneficial as this may be for business, this utilitarian calculus lacks an understanding of how and why data privacy is important not only to the human pocketbook, but to human dignity and autonomy.

In contrast, the Directive gives birth to informational privacy not via the language of the market, but through the language of rights, reflecting both the European Convention on Human Rights[15] and the UN Universal Declaration of Human Rights.[16] It is a treatment based on a deeper moral argument, one perhaps closer to Warren and Brandeis' notion of the "right to one's personality," even if made in an entirely different context. It argues that privacy includes a significant level of control over personal information, and while this may indeed be beneficial in reducing transaction costs and increasing consumer confidence, non-economic interests inform the bulk of the reasons for the existence and extent of this control. Proponents of this "deeper" understanding of data privacy argue that control over personal information is a necessary component of human dignity and autonomy.

While Warren and Brandies did not explicitly define what the "right to one's personality" was, they seem to suggest that there is some core of the self that ought to be protected by privacy. This is a commonly held position, though not there is dispute over the phrasing and over what precisely the "core" of a person is. Bloustein, for example, believes that "inviolate personality" "defines man's essence as a unique and self-determining being" and that "this is in some sense a spiritual interest rather than an interest in property or reputation."[17] When privacy violations threaten to damage the "inviolate personality" of individuals, he argues, the law needs to respond in order to protect human dignity and individuality.[18] For Reiman, privacy is "a social ritual by means of which an individual's moral title to his existence is conferred."[19] By this, I take him to mean that being granted privacy rights allows individuals to understand that some aspects of the self are theirs, and theirs alone, and this understanding is key to individuals seeing themselves as, in fact, "individuals." Reiman argues that individuals "must recognize that [they] have exclusive moral rights to shape [their] destiny."[20] Privacy violations, therefore, are those that "penetrate the private reserve of the individual" and "[destroy] the self."[21] Wasserstrom agrees, suggesting that one plausible conception of what it is to be a person is "the idea of an existence of a core of thoughts and feelings that are

---

15 *European Convention for the Protection of Human Rights and Fundamental Freedoms*, 4 November 1950, 213 U.N.T.S. 221 at 223, Eur. T.S. 5 [ECHR], Art. 8.

16 *Universal Declaration of Human Rights*, G.A. Res. 217A (III), U.N. Doc. A/810 at 71 (1998).

17 Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 156–202 at 163, 187.

18 *Ibid.* at 178.

19 Jeffrey H. Reiman, "Privacy, Intimacy, and Personhood" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 300–316 at 310.

20 *Ibid.*

21 *Ibid.* at 311.

a person's alone," and so the required disclosure of these thoughts and feelings diminishes personhood; privacy, therefore, protects against such disclosure.[22] Moore argues that we ought to recognize a moral claim to control personal information (and also control over access to oneself), because privacy is a "cultural universal necessity for our proper functioning."[23]

Schoeman also believes that, in general, the protection of the self is a desirable thing and that privacy "marks out something morally significant about what it is to be a person."[24] He argues that there is evidence to suggest that privacy allows individuals to express the different dimensions of the self, not in the sense of multiple-personality disorders, but rather in the sense that behaviour is not consistent, and shifts across contexts.[25] The notion of the protection of the self is conceptually similar to notions of dignity, or respect for persons. Respecting human dignity means, partially, respecting individuals as persons and, to that extent, it overlaps with protection of the self or personhood. However, personhood refers exclusively to the state of an individual — it is concerned with one person's thoughts, beliefs, freedoms, etc. In contrast, the concept of dignity implies concern not only for the status of a single being, but also for the relationships in which he is embedded. In other words, "personhood" is a state that an individual has, lacking a concern for how that state is necessarily obtained, while "dignity" can only be achieved if one is *treated* with dignity by others; dignity is, therefore, premised not only on the individual, but also upon relationships. For Miller, then, "our sense of dignity derives from our right to be individuals while co-existing in one society."[26] For Post, "dignity depends upon intersubjective norms that define the forms of conduct that constitute respect between persons."[27] Benn also recognizes the relational component of dignity, suggesting that, according an individual, dignity means respecting her as an actual or potential "chooser," an individual attempting to navigate her own course through life.[28] Respecting dignity, therefore, requires us "to take account of the way in which [another individual's] enterprise might be affected by [our] own decisions."[29]

---

22 Richard A. Wasserstrom, "Privacy: Some Arguments and Assumptions" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 317–345 at 322.

23 Adam D. Moore, "Toward Informational Privacy Rights" (2007) 44 San Diego L. Rev. 809 at 817.

24 Ferdinand David Schoeman, "Privacy and Intimate Information" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 403–418 at 404.

25 *Ibid.,* at 410.

26 Jeremy A. Miller, "Dignity as a New Framework Replacing the Right to Privacy" (2007) 30:1 Thomas Jefferson L. Rev. 1 at 2

27 Robert C. Post, "Three Concepts of Privacy" (2000) 89 Geo. L.J. 2087 at 2092.

28 Stanley I. Benn, "Privacy, Freedom, and Respect for Persons" in F. D. Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (New York: Cambridge University Press, 1984) 223–244 at 229.

29 *Ibid.*

Fried claims that choosing what to reveal about ourselves goes to the core of our ability to engage fully with others, arguing that "privacy in its dimension of control over information is an aspect of liberty . . . [but also] is the necessary context for . . . relationships of love, friendship, and trust."[30] But, the freedom to engage must also imply the freedom to withdraw — Bloustein is concerned with the damaging effects that a lack of privacy can have on the human psyche, arguing that to be human means to have the ability to shield elements of one's life from the gaze of others:

> [T]he man who is compelled to live every minute of his life among others and whose every need, thought, desire, fancy or gratification is subject to public scrutiny, has been deprived of his individuality and human dignity.[31]

The EU Directive is premised on a similar understanding of informational privacy's normative function — the idea that when information is gathered about our habits, preferences, and lifestyles, and is processed without our consent or knowledge in order to slice us into particular demographics, target markets, and threat profiles, we are deprived of our individuality and dignity. Recognising this means abandoning a market-driven approach to informational privacy as it posits that, while there may, indeed, be costs to business associated with a strong right to informational privacy, non-economic reasons outweigh these costs. Since it comes from the liberal language of rights and dignity, it is not surprising that the Directive creates a regulatory model that places the bulk of control over what kinds of information can be held and processed, and for what purposes, in the hands of the individuals who make up the source of that information.

In contrast, market-oriented approaches such as the APEC Framework offer only limited control over personal information to individuals and, therefore, do not draw on the same normative groundings of a claim to privacy. When some control over information is granted, it tends to be done so for the purposes of something resembling consumer protection, rather than out of a desire to protect privacy. This reflects an understanding of informational privacy that sees a degree of control over personal information as a potentially beneficial interest for consumers, but one that may often come at too high an economic price for business. As a result, substantive protections in market-oriented models are relatively low and contain a significant number of built-in exemptions, and there are no strong procedural mechanisms to guarantee their enforcement. In contrast, rights-based models, such as the Directive, treat privacy in personal information as a fundamental right that should only be limited in the most serious of instances, and ensure that this right is overseen on a national level in each member State by an independent public data commissioner and enforced by appropriate judicial mechanisms.

The gap between the protections that come out of these two normative approaches to informational privacy is significant. When comparing the EU Data Protection Directive and the APEC Privacy Framework, it soon becomes clear that Framework cannot be considered an "adequate" data protection regime as contemplated by Article 25 of the Directive, because of this normative gulf. Absent con-

---

30 Fried, *supra* note 9 at 483-484.

31 Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser" (1964) 39 N.Y.U. L. Rev. 962 at 1003.

tractual agreements of the sort envisaged by Article 26,[32] the transfer of personal data from EU Member states to organisations in third states with privacy laws modelled up on the APEC Framework ought, therefore, to be prohibited.

## II. THE APEC PRIVACY FRAMEWORK

### (a) Background

The APEC Framework was the culmination of more than five years of negotiation between APEC Member economies on the protection of personal data within the region. In 1998, APEC announced a broad plan to use information technology to assist regional economies in modernising. This included an agreement that:

> Government and business should co-operate to develop and implement technologies and policies, which build trust and confidence in safe, secure and reliable communication, information and delivery systems, and which address issues including privacy, authentication and consumer protection.[33]

The following year APEC established the Electronic Commerce Steering Group (ECSG) in order to help realise these goals. The ESCG created a Data Privacy Subgroup in 2003, which released a draft of the APEC Framework in 2004; APEC Ministers formally approved the APEC Framework the following year.

The Preamble to the APEC Framework states that the APEC Member economies recognise "the importance of protecting information privacy and maintaining information flows among economies in the Asia-Pacific region and among their trading partners."[34] It soon becomes clear from the rest of the Preamble that the focus of the whole APEC Framework is squarely on maintaining those valuable flows. Informational privacy is envisioned as a positive thing only insofar as it does not jeopardize economic growth; its purpose is "to improve consumer confidence and ensure the growth of electronic commerce."[35] Indeed, the Preamble is careful to note that overly rigorous protections may have "adverse implications for global business" and, therefore, any data protection regime must "account for [this] new realit[y]."[36] This normative approach to informational privacy treats it as useful for the purposes of consumer protection, eschewing the language of "rights" entirely; this has dramatic consequences for both the substantive and procedural components

---

32 Art. 26(2):

> [...] 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.

33 APEC, *APEC Economic Leaders Declaration: Strengthening the Foundations for Growth* (18 November 1988) at 16, online: Asian LII <http://www.asianlii.org/apcc/other/agrmt/6aeldstffg689>.

34 *APEC Framework*, *supra* note 3, Part i(1).

35 *Ibid.*

36 *Ibid.*, Part i(3).

(outlined in the following section) of the APEC Framework, ultimately meaning it cannot be considered "adequate."

## (b) Structure of the APEC Framework

### *(i) Substantive Protections*

The APEC Framework groups its substantive provisions under nine broad headings: preventing harm, notice, collection limitation, uses of personal information, choice, integrity of personal information, security safeguards, access and correction, and accountability.[37]

#### (A) Preventing Harm

Individuals have a legitimate expectation of privacy in their personal information, and protections should be designed to prevent harm to individuals because of the wrongful collection or misuse of that information. Remedies for privacy infringements ought to be designed to prevent further harm to individuals and should be proportionate to the likelihood and severity of the threat that exists because of the use of that information.

#### (B) Notice

Individuals should be able to know what information is collected about them and for what purpose it is used. Holders of collected information are to take all reasonably practicable steps to ensure that notice is provided either before or at the time of collection of the information, or if this is not possible (for example, where the information is not obtained directly, but through a third party), as soon after as is practicable. It is not necessary to give notice where the information in question is in the public domain, or is information that identifies an individual in a professional capacity.

#### (C) Collection Limitation

The collection of information must be limited by reference to the purposes for which it is collected. Collection must be relevant to the stated purposes, and collection methods must be lawful and fair and conducted with notice to, or the consent of, the individual concerned. There are, however, circumstances in which providing notice to, or obtaining consent of, individuals would be inappropriate, such as during a public health emergency.

#### (D) Uses of Personal Information

Personal information can only be used to fulfil the purposes of collection and other compatible or related purposes. However, information can be used for different purposes than those stated during collection in three circumstances — with the consent of the individual, where it is necessary to provide a product/service requested by the individual, or by the authority of law. A compatible or related pur-

37 *Ibid.*, Part iii(I-IX).

pose is to be determined by asking whether the extended usage stems from, or is in furtherance of, the original purpose of collection.

(E) Choice

Individuals are to be provided with choice in relation to the collection, use, transfer, and disclosure of their personal information, to be exercised through clear, accessible, easily understandable, and affordable mechanisms. These mechanisms may not be necessary where the information is collected from the public domain, or in relation to information that identifies an individual in a professional capacity, or in certain employer-employee relationships.

(F) Integrity of Personal Information

There is an obligation on holders of collected personal information to maintain the accuracy and completeness of records, to the extent necessary for the purposes of the use of the information.

(G) Security Safeguards

Individuals are entitled to expect that their information is protected. Safeguards should be proportional to the likelihood and severity of the harm threatened, the sensitivity of the information and the context in which it is held, and should be subject to periodic review.

(H) Access and Correction

While the ability to access and correct information held about oneself is a central aspect of privacy protection, it is not an absolute right. Individuals should be able to obtain from the information controller confirmation about whether information is being held about them, have that information communicated to them (within a reasonable time and in a reasonable manner), challenge the accuracy of that information and (if appropriate) have it rectified or deleted. However, access and opportunity for correction may not be provided where the burden or expense of doing so would be disproportionate to the risks to the individual's privacy; this is so where there are legal or security concerns, to protect confidential commercial information, or where access would violate the informational privacy of third parties. If a request for access is denied, the individual should be provided with reasons for the denial and an opportunity to appeal.

(I) Accountability

Personal information controllers should be accountable for complying with measures taken to give effect to the principles embodied by the APEC Framework. When personal information is to be transferred, the controller should obtain the consent of the individual or take reasonable steps to ensure that the recipient will protect the information in a manner consistent with the APEC Framework.

***(ii) Procedural Protections***

Of course, as a policy document the APEC Framework is not legally enforceable on its own, but even if we were to imagine it being implemented as domestic

legislation in a APEC Member economy, it does not prescribe the procedural protections necessary to ensure individuals could enforce their rights. Indeed, it specifically suggests that a Member economy could implement the substantive provisions in any manner it saw fit.[38] This is a significant weakness and, again, reflects a normative conception of informational privacy as primarily a market-oriented regulatory tool rather than as a human right.

## III. THE EU DATA PROTECTION DIRECTIVE

### (a) Background

Western Europe has a comparatively long history of data protection laws, culminating with the Directive. The OECD Privacy Guidelines represented the first transatlantic bargain related to privacy protections for personal data; OECD member nations were to follow them when developing their own national legislation.[39] However, practice did not follow theory and differing interpretations of these principles between the United States and a number of the European nations led to diverging data privacy standards. The European Council subsequently tightened standards in Europe by essentially making the OECD guidelines enforceable, requiring countries to establish both sanctions and remedies for informational privacy violations;[40] the Directive specifically acknowledges that it is designed to amplify the protections agreed upon by the Council.[41] It is telling that the APEC Framework bears a strong resemblance to the OECD guidelines that Europe deemed insufficient.

### (b) Structure of the EU Data Protection Directive

The Directive lays out its priorities early on and relies on the language of rights to do so. The recital stresses that "data-processing systems are designed to serve [people] . . . [and] must respect their fundamental rights and freedoms, notably the right to privacy."[42] While acknowledging that "personal data should be able to flow freely from one Member State to another," the recital notes that this should only occur where the "fundamental rights of individuals" are safeguarded.[43] Both the substantive and procedural protections of the Directive are far more stringent than those envisaged by the APEC Framework, reflecting a deep concern for informational privacy that extends beyond any economic benefit it may bring through an increase in consumer confidence. This evidences an important difference in the purposes of the APEC Framework and the Directive; even though the Directive

38 *Ibid.*, Part iv.

39 OECD, *Guidelines on the Protection of Privacy and Transborder Flows of Personal Data* (1980), online: OECD <http://www.oecd.org/document/20/0,3343, en_2649_34255_15589524_1_1_1_1,00.html>.

40 Council of Europe, *Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data*, 28 January 1981, ETS-108, online: Council of Europe <http://www.conventions.coe.int/treaty/en/treaties/Html/108.htm>.

41 *Directive*, *supra* note 2, 11th recital.

42 *Ibid.*, 2nd recital.

43 *Ibid.*, 3rd recital.

acknowledges the economic value of processed data, "it is not easy to extract from [the] Directive any purpose other than the protection of privacy."[44] The Directive does not dispute that data flows have important economic benefits; indeed, it encourages such flows. However, it aims to ensure that both the collection and processing of the data that makes up those valuable flows takes place in accordance with strict guidelines, including an attempt to ensure that switching jurisdictions cannot circumvent those guidelines. While "cross-border flows of personal data are necessary to the expansion of international trade," the importance of informational privacy *as a right* means that "the transfer of personal data to a third country which does not ensure an adequate level of protection must be *prohibited*."[45]

### *(i) Chapter I — General Provisions*

The opening Chapter outlines the objective and applicability of the Directive, along with the definitions of terms of art it uses. It notes that the Directive applies to all processing of personal data wholly or partially by automatic means, but there are exceptions for household activity, national security, criminal law, etc. The object of the Directive is to "protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy with respect to the processing of personal data."[46] From the start then, the emphasis of the Directive is squarely on privacy rights rather than economic growth, and this positions the right to data privacy as something much more than a regulatory tool.

### *(ii) Chapter II — General Rules on the Lawfulness of the Processing of Personal Data*

Chapter II contains the substantive rules relating to the processing of personal data that the Directive requires Member States to adopt, and is divided into nine sections.[47] When compared to their counterparts in the APEC Framework, the Directive's substantive principles are more detailed, create broader rights, and contain fewer exemptions.

#### Section I — Principles Relating to Data Quality

Member States must provide that all personal data for specific purposes is processed lawfully and fairly — that it is adequate, relevant, and not excessive, and is kept in a form that permits the identification of data subjects for no longer than is necessary.

#### Section II — Criteria for Making Data Processing Legitimate

Personal data can be processed only if the data subject has given her consent, except in particular defined scenarios (i.e. it is necessary for the performance of a

---

44 *Johnson v. Medical Defence Union Ltd.*, [2007] EWCA Civ 262, ¶16, Buston L.J (C.A.).

45 *Directive*, *supra* note 2, 56th and 57th recitals [emphasis added].

46 *Ibid.*, Ch. I, Art. 1.

47 *Ibid.*, Ch. II, Arts. 5–21.

contract to which the subject is party, or is necessary for compliance with legal obligations, etc.).

### Section III — Special Categories of Processing

The processing of personal data revealing ethnicity, political opinions, religious beliefs, trade-union membership, or relating to the subject's health or sex life is prohibited except in particular defined scenarios. Member states are required to provide exemptions for the processing of personal data carried out solely for journalistic purposes or the purpose of artistic/literary expression where it is necessary to reconcile the right of privacy with rules governing freedom of expression.

### Section IV — Information to be Given to the Data Subject

Data controllers must provide data subjects with their identity, the purposes of the processing, and any other information that is necessary to guarantee fair processing. Where the data about the subject was not obtained from the subject, the controller must disclose this same information to the subject no later than the time when the data was first disclosed to the controller.

### Section V — The Data Subject's Right of Access to Data

The data subject has the right to obtain from the controller confirmation of data held about the subject that is being processed and its purposes, the end recipients of this data, the source of the data, and the logic involved in any automatic processing in the case of automated decisions made about the subject. The data subject also has the right to block or rectify the processing of data that does not comply with the Directive, and to require the controller to inform any third parties who have already received the data of this block or rectification, so long it does not prove impossible or require disproportionate effort.

### Section VI — Exemptions and Restrictions

Member States may choose to adopt legislative measures to restrict the scope of the obligations and rights under the Directive when necessary to safeguard certain vital interests (national security, the rights and freedoms of others, etc.).

### Section VII — The Data Subject's Right to Object

The data subject may object to the processing of personal data in certain circumstances (i.e. where the data is processed for the purposes of direct marketing). Member States are required to grant to every person the right not to be a subject of a decision based solely on automated processing of data where that decision produces legal effects or is of significant effect.

### Section VIII — Confidentiality and Security of Processing

Data controllers must implement appropriate technical and organisational measures in order to protect personal data against destruction, loss, or unauthorised disclosure or access.

Section IX — Notification

Any data controller must inform the relevant public supervisory authority prior to carrying out any processing operation, except in certain specified conditions. The controller must provide information regarding the purpose of the processing, the type of data to be processed, the end recipients of the data, and any proposed transfer outside the European Union. Member States shall determine the risks any processing operation might pose, prior to the start of that operation, by means of checks carried out by the public authority upon receipt of notification from a controller. All processing operations should be publicized and listed in a public registry.

### *(iii) Chapters III–VII (excluding Chapter IV)*

The remaining chapters are largely procedural. Chapter III deals with judicial remedies, liability, and sanctions for any breach of the Directive's provisions. Chapter V directs Member States to draw up relevant codes of conduct for controllers to follow. Chapter VI mandates the creation of a fully independent public authority (i.e. a national Data Protection Commissioner) responsible for monitoring the application of the Directive in their respective Member States. These authorities are to have investigative and enforcement powers, and the power to engage in legal proceedings. Chapter VII outlines how the Directive is to be implemented.

### *(iv) Chapter IV: Transfer of Personal Data to Third Countries*

> The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if . . . the third country in question ensures an adequate level of protection.[48]

Where the Commission finds that the protection offered by third countries is not "adequate," Member States are required to take measures necessary to prevent the transfer of personal data to the third country in question, except in a limited range of circumstances.[49] Adequacy is to be assessed on a case-by-case basis, and to this end Article 29 creates a standing "Working Party on the Protection of Individuals with regard to the Processing of Personal Data" (hereafter, the "Working Party") tasked with the responsibility of, *inter alia*, giving the Commission opinions on the level of protection in third countries. The Commission is not obliged to accept the recommendations of the Working Party, though clearly they carry great weight and the Commission is required to inform the Working Party of the action it has taken in response to its reccommendations.

## IV. ANALYSIS: IS THE APEC FRAMEWORK "ADEQUATE" UNDER THE WORKING PARTY'S APPROACH?

The Working Party follows a two-stage process in making a determination of adequacy: an analysis of the content of the rules applicable, and an analysis of the

48 *Ibid.*, Ch. IV, Art. 25.

49 *Ibid.*, Ch. IV, Art. 26.

means for ensuring their effective application.[50] Therefore, for a non-EU data protection regime to be considered adequate, it must meet a core of substantive and procedural principles.

While adoption of the Framework by APEC Member economies is voluntary, let us hypothetically assume that a Member economy currently lacking *any* data protection legislation implemented the provisions of the APEC Framework into their domestic legal order. Is it possible that such legislation could be considered "adequate" within the meaning of Article 25, following the Working Party's analytical framework? Unless a Member economy voluntarily decided to upgrade their data protection laws beyond that required by the APEC Framework, the following analysis suggests that the answer is "no." The APEC Framework, as it stands, sets a relatively low threshold for data protection laws, and does not conform to a majority of either the substantive or procedural requirements of the Working Party for a finding of adequacy.

## (a) Core Substantive Principles Required for a Finding of "Adequacy" by the Working Party

The Working Party will only find a third-state data protection regime to be "adequate" within the meaning of Article 25 when it finds that it complies with the following substantive principles: data is collected for limited and defined purposes; data is of sufficient quality and is used proportionally for the purposes for which it was collected; there is transparency about any collection and processing; there are sufficient security measures; there are appropriate rights of access, rectification, and opposition; there are rules regarding onward transfers; and there are particularly stringent rules in special defined circumstances.

### *(i) The Purpose Limitation Principle*

The Working Party has said that data should be processed for specific purposes and only subsequently used in a manner not incompatible with those purposes, except where an exemption could be justified as necessary in a democratic society.

Principle IV of the APEC Framework deals with the uses to which collected personal data can be put, holding that it may only be used to fulfil the purposes of collection and other related or compatible purposes. The commentary to the APEC Framework states that:

> [T]he fundamental criterion in determining whether a purpose is compatible with or related to the stated purposes is whether the extended use stems from or is in furtherance of such purposes.[51]

---

50 European Commission (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), *Working Document on the transfers of personal data to third countries: Applying Articles 25 and 26 of the EU data protection directive*, (1998) DG XV D/5025/98 at 5, online: European Commission <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1998/wp12_en.pdf> [Working Document].

51 *APEC Framework*, *supra* note 3, Part iii(IV)(19)(commentary).

On the surface, then, the APEC Framework would seem to conform to the requirements of the Purpose Limitation Principle, although there may be some concern regarding some of the exemptions. While the Working Party has stated that the only acceptable exemptions are the sort to be found in Article 13 of the Directive[52] the APEC Framework includes seemingly less serious exemptions, such as where an individual consents to unrelated uses, or when the unrelated use is necessary to provide a product or service requested by a data subject. Such business-friendly exemptions should alert us to the nature of the APEC Framework — it is designed to provide fairly minimal standards of data protection that are enough to enhance consumer confidence, but do not hamper the economic benefits of the free flow information. In contrast, the Directive seeks to ensure that personal data can only be used for a different purpose from that for which it was collected in situations that are of serious public concern, reflecting the importance with which it treats informational privacy as a human right.

### *(ii) The Data Quality and Proportionality Principle*

To comply with this principle, the APEC Framework would have to ensure that personal data is accurate and (where necessary) up-to-date, relevant, and not excessive in relation to the purposes for which it is being processed. The relevant Framework provision here is Principle VI, which relates to the integrity of personal information, requiring it to be accurate, complete, and kept up-to-date to the extent necessary for the purposes of use. It seems likely that this is sufficient to meet the Working Party's requirements. However, it is notable that there is no requirement placed on data controllers to delete information that is no longer required; the removal of outdated information would be the responsibility of the data subject, under the right of access and rectification.

### *(iii) The Transparency Principle*

To comply with this core principle, the APEC Framework must ensure that individuals are provided with notification about the collection and processing of their personal data, the identity of the data controller, and any other information required to ensure fairness, subject only to limited exceptions similar to those in Articles 11(2) and 13 of the Directive.[53] The relevant Framework provision here is Principle II, regarding notice. It holds that individuals should receive notice when

---

52 Under Art. 13, Member states may adopt exemptions where necessary for purposes of national security, defence, public security, the prevention/detection/investigation/prosecution of criminal offences or breaches of ethics for regulated professions, important state-level economic or financial interests, a monitoring/inspecting/regulating function connected with the exercise of official authority in defined circumstances, and the protection of a data subject or any individual's rights.

53 Under Article 11(2), where the data was not obtained from the individual directly, no disclosure to the individual is required where in particular for processing for statistical purposes or for the purposes of historical or scientific research, the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by law (though appropriate safeguards must still be created).

their personal information is being collected, the purpose of the collection and who will receive the information, the identity and location of the data controller, etc. While this initially appears to conform to the Working Party's requirements, there are two concerns: one regarding the timing of the notice requirement, the other regarding a series of exemptions granted to the processing of publicly-sourced information.

Under the Directive, notice is to be given to the data subject at the time of collection of the data (that is, prior to processing).[54] Under the APEC Framework, in contrast, it is possible for notice to be given "as soon after [collection] as is practicable."[55] The commentary to the APEC Framework adds that the decision of when precisely to provide notice should be "based on a consensus among APEC Member economies."[56] Pounder points out that this consensus could very well be one of commercial convenience rather than of fair treatment of data subjects.[57] If this were the case, then the entire notice principle is diminished in value, and suggests that the APEC Framework fails to meet the Working Party's core requirement of transparency.

The exemptions listed in the APEC Framework also create problems for transparency: it notes that it "may not be appropriate for personal information controllers to provide notice regarding the collection and use of publicly available information."[58] Similarly, Principle V, which holds that individuals should be provided with mechanisms to enable them to exercise choice in relation to the use and disclosure of their personal information, contains an exemption for data collected from publicly available sources. Such exemptions for publicly-sourced information are ill-advised because they fail to recognise the impact that exponential growth in computing power will have on the processing of data. The increasing use of computers to link previously disparate pieces of publicly available information and the rapidly developing field of facial recognition poses new threats to personal privacy that such exemptions do not recognise. For example, it is likely that under the APEC Framework it would be entirely acceptable to compile a database that tracks individuals as they are photographed on CCTV systems travelling through public spaces, and tie this into any data they have provided about themselves on the Internet, and not require any consent from the individuals in question. In contrast, under the Directive and similarly comprehensive legislation, the vast majority of publicly sourced information is still protected by the relevant privacy principles. While information taken from a publicly-run and accessible register (i.e., a collec-

54 *Directive*, *supra* note 2, Ch. II, s. IV, Art. 10.

55 *APEC Framework*, *supra* note 3, Part iii(II)(16).

56 *Ibid.*, Part iii(II)(15–17) (commentary).

57 Chris Pounder, "Why the APEC Privacy Framework is Unlikely to Protect Privacy" Data Protection Quarterly, (2007) online: Out-law.com <http://out-law.com/default.aspx?Page=8550>.

58 *APEC Framework*, *supra* note 3, Part iii(II)(17).

tion of census records) is not protected,[59] the collection and processing of photographs taken in public places would likely activate the Directive's protections.[60]

In its analysis of Argentina's privacy regime, the Working Party criticized an exemption to the consent requirement for publicly-sourced information similar to that found in the APEC Framework, stating it would only be acceptable if there were additional rules that guaranteed that the processing of data from public sources would not constitute a threat to the fundamental rights and freedoms of individuals, particularly their right to privacy.[61] There are, however, no similar additional rules found in the APEC Framework that might serve as backup (for example, by differentiating between different kinds of publicly-available data and requiring notice/consent for certain types). The broader exemptions exist because they are not seen as impacting upon the ability of the individual to participate in the marketplace and, therefore, are of little concern to the APEC Framework's drafters.

### *(iv) The Security Principle*

This Working Party requires that sufficient technical and organisational security measures be present given the nature of the processing in question. Principle VII of the APEC Framework requires that data controllers protect the personal information they hold against risks such as loss or unauthorized access, and the safeguards should be proportionate to the likelihood and severity of the harm threatened. This would seem to conform to the requirements of the Directive.

### *(v) The Rights of Access, Rectification, and Opposition*

For the APEC Framework to meet this core requirement, as outlined by the Working Party, it would have to ensure that the data subject has the right to obtain a copy of any of their personal data that is being processed, and a right to correct any errors in that data, subject only to the type of exemptions found in Article 13 of the Directive, above. The relevant Framework principle is Principle VIII, which relates to access and correction. Again, on the surface, it appears as though the APEC Framework meets the requirements of the Directive, but the exemptions it grants raise concerns. Principle VIII *does* provide that individuals should be able to receive copies of their personal information from a data controller in a reasonably fast and non-cost prohibitive manner, and further that they should be able to challenge the controller when errors are discovered. If the APEC Framework ended at

---

59 *Directive*, *supra* note 2, Ch. IV, Art. 26(1)(f).

60 This is an area of increasing concern; see for example a letter from the Privacy Commissioner of Canada to Google outlining her concerns regarding the automatic photographing of individuals under Google's "Streetview" Mapping Service, online: Office of the Privacy Commissioner of Canada <http://www.priv.gc.ca/media/let/let_070911_01_e.cfm>.

61 The Working Party concluded that Argentina did, in fact, provide such additional rules. European Commission (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), *Opinion 4/2002 on the level of protection of personal data in Argentina* (2002) 11081/02/EN/Final, at 16-17, online: European Commission <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2002/wp63_en.pdf> (last accessed 14 May 2009) [WP Opinion on Argentina].

that point, all would likely be well from the perspective of determining adequacy. However, the APEC Framework goes on to list several exemptions from the right of access and notification.

While the Working Party has stated that limited exemptions for matters of national interest are acceptable in this context, the APEC Framework conceives of a broader exemption in any situation where the burden or expense of allowing access and correction would be "disproportionate" to the risks to the individual's privacy. Pounder notes that these exemptions tie into the APEC Framework's "preventing harm" principle, under which any available remedial measures and specific obligations upon data processors are to be proportionate to the likelihood and severity of the harm threatened by the collection.[62] Pounder argues that this means that where data processors do not perceive any particular harm to be likely, then the exemptions in the APEC Framework (such as not requiring notice or access) come into play, resulting in a counter-intuitive scenario:

> Access by the data subject to his or her own personal data can be refused if there is little risk of harm to the data subject, yet the reason why the data subject might want to seek access is to find out whether the processing is causing him harm.[63]

Pounder notes that other data protection regimes, including the Directive, reject this approach, and instead assume that it is the data *subject* that is best placed to assess the risk of harm because the sensitivity of the data in question is a "subjective assessment that [can] only be accurately judged by [the] data subject."[64] The APEC Framework seems to place greater emphasis on the needs of data processors rather than on the rights of the data subjects and this, again, reflects a different normative interpretation of informational privacy. The authors of the APEC Framework seem to dispute that individuals have any deep and meaningful concern in preventing the circulation of erroneous information about them because there is no perceived impact on consumer confidence or on marketplace behaviour.

### *(vi) Restrictions on Onward Transfers*

The Working Party requires that further transfers of personal data by the recipient in the third country be permitted only where the next jurisdiction *also* features data protection rules that are "adequate," subject to exceptions similar to those outlined in Article 26 (above). This is, of course, necessary to ensure that the protections required by the Directive cannot be circumvented through multiple transfers to jurisdictions with increasingly weaker data protection regulations. The Working Party does not require something as rigorous as Article 25 in order to meet this requirement. APEC could meet it by simply requiring individual contractual measures ensuring adequate levels of protection for onward transfers are guaranteed, as is done in Article 26 of the Directive, in addition to both the Safe Harbor agreement

62 *APEC Framework*, *supra* note 3, Part iii(I)(14).

63 Pounder, *supra* note 57.

64 *Ibid.*, Pounder referring to the Lindrop Committee Report on Data Protection (Cmnd 7341, paras. 18.24–18.27).

and the Canadian data protection regime, PIPEDA.[65] The APEC Framework, however, contains no rules whatsoever about onward transfer. Under the "Guidance for International Implementation" provisions, Member economies are merely encouraged to develop cross-border privacy rules that adhere to the Principles of the APEC Framework, so long as they do not create "unnecessary administrative and bureaucratic burdens for business and consumers."[66]

### *(vii) Special Situations*

The Working Party has identified three situations in which additional protections may be required beyond these core substantive principles; these are situations involving the processing of sensitive data, direct marketing, and automated individual decisions. Sensitive data is data that reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, health or sexual information, or information relating to criminal records.[67] Where this sort of data is involved, the Working Party requires that additional safeguards (such as explicit consent) be in place. In the case of direct marketing, the individual should be able to opt-out entirely of the processing of their data for such purposes. In the case of automated individual decisions, the Working Party requires that the individual should have the right to know the logic involved in the decision, and that other (unspecified) measures should be taken to safeguard the individual's legitimate interest.

The APEC Framework makes no distinction between different kinds of personal information, however, simply defining it as "any information about an identified or identifiable individual."[68] Faced with a similar lack of distinction in its analysis of the Canadian data protection regime, the Working Party found that provisions in the Canadian legislation requiring organisations to take into account the "sensitivity" of the data in question nonetheless met the requirement of adequacy.[69] Yet the APEC Framework falls short on this approach too, subsuming all personal information into a single type and stating only that "where appropriate, individuals should be provided with [the ability] to exercise choice in relation to the use of that data."[70]

The APEC Framework makes no reference whatsoever to any special provisions for the use of personal information in direct marketing, in contrast to the Working Party which argues that an individual ought to be able to opt out of any such use — given the general pro-business orientation of the APEC Framework,

---

65 *The Personal Information Protection and Electronic Documents Act*, S.C. 2000, c. 5, sched. 1, cl. 4.1.3 [*PIPEDA*].

66 *APEC Framework*, *supra* note 3, Part iv(B)(III)(48).

67 *Directive*, *supra* note 2, Ch. II, Art. 8.

68 *APEC Framework*, *supra* note 3, Part ii(9).

69 European Commission (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), *Opinion 2/2001 on the adequacy of the Canadian Personal Information and Electronic Documents Act* (2001) 5109/00/ENat 3-4, online: European Commission <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2001/wp39_en.pdf> [WP Opinion on Canada].

70 *APEC Framework*, *supra* note 3, Part iii(V).

this is unsurprising. Again, it is possible that such an option could be included within the broader "choice" provisions of the fifth Framework principle, but it is not specified. Finally, the APEC Framework makes no reference to the third special case identified by the Working Party — automated decision making within the meaning of Article 15 of the Directive.

## (b) Core Procedural Principles Required for a Finding of "Adequacy" by the Working Party

While in the EU data protection principles are implemented via statute and supervised by an independent authority, this is not always the case elsewhere. Acknowledging this, the Working Party has developed a scheme to allow a determination of the adequacy of procedural measures in both judicial and non-judicial contexts in third countries, based on three core objectives — good rule compliance, the provision of assistance to data subjects in exercising their rights, and the provision of appropriate redress to subjects who have suffered violations of the rules.

### *(i) Good Compliance with the Rules*

A lack of judicial enforcement will not necessarily prevent a finding of adequacy so long as there is generally good compliance with the rules that relate to the enforcement of the substantive core principles. While no system is likely to achieve 100% compliance with the rules, a good system is "characterised by a high degree of awareness among data controllers of their obligations, and among data subjects of their rights."[71] Of course, the existence of effective sanctions and/or direct verification by independent public authorities goes a long way toward creating such a good system.[72]

Since the APEC Framework is neither legally enforceable on its own accord, nor creates any independent data protection authorities, does it, nonetheless, have the potential for creating good rule compliance? Again, we must consider a hypothetical scenario in which an APEC Member economy implements the APEC Framework as domestic legislation. Part IV of the APEC Framework outlines various options that Member economies might take in implementing the Principles, and gives tremendous deference to whichever means an individual Member economy might feel is most appropriate, including the use of central authorities, multi-agency enforcement bodies, self-regulation via a network of designated industry bodies, or any combination thereof.[73] Flexibility is the name of the game, and so there is no guarantee that a Member economy that did incorporate the APEC Framework into domestic law would create a system that ensured effective rule compliance.

The APEC Framework fails to identify any specific administrative or criminal sanctions, though it does note that there should be "remedial measures . . . proportionate to the likelihood and severity of the harm" caused by inappropriate collec-

71 WP Working Document, *supra* note 50 at 7.

72 WP Opinion on Argentina, *supra* note 61 at 13–16.

73 *APEC Framework*, *supra* note 3, Part iv(A)(31).

tion or use of personal information.[74] Indeed, the APEC Framework shies away from encouraging the creation of robust sanctions, suggesting only that systems for providing privacy protections *may* include rights of legal enforcement.[75] There is, however, recognition in the APEC Framework that it must be known and accessible for it to have any meaningful effect and, to this end, suggests that Member economies ought to publicise the relevant privacy protections to the citizenry, educate data controllers about the protections, and educate individuals as to how they can exercise their rights.[76]

Of course, this is merely a hypothetical scenario and it is impossible to judge effective compliance with the rules until they are domestically incorporated on some level. However, one can make the broad proposition that the lack of any *required* enforcement mechanisms is likely to undercut the potential the APEC Framework has for ensuring good compliance with the substantive rules, and this is likely to militate against a future finding of adequacy.

### *(ii) Provision of Assistance to Individual Data Subjects*

The Working Party has said that it is a fundamental requirement of an adequate data protection regime that individuals be able to enforce their rights in a prompt and effective manner, and not be burdened by undue costs in doing so. There must be an independent institutional mechanism that data subjects can utilize in order to enforce their rights.

While the APEC Framework requires that the Principles it contains be known and accessible, and while this may indeed help individuals exercise their rights, it falls far short of the institutional requirement spoken of by the Working Party. While a central authority could theoretically be used to implement the APEC Framework's principles, it is not required as such, and the APEC Framework stresses that different Member economies may "determine that different [Principles] may call for different means of implementation" and, therefore, it is important to be "respectful of the requirements of [Member economies]."[77]

### *(iii) Provision of Appropriate Redress*

The Working Party has identified the capability of a data protection regime to provide appropriate redress to the injured party following breach of the rules to be a "key element"; one which "must involve a system of independent adjudication or arbitration" that can either provide compensation or impose sanctions.[78] The APEC Framework does not require the creation of such an independent system, and specifically provides for flexibility in implementation, as mentioned above. However, the Working Party has accepted that the absence of specific rules regarding redress in a data protection regime may, nonetheless, be acceptable where there are residual

74 *Ibid.*, Part iii(I)(14).

75 *Ibid.*, Part iv(A)(38).

76 *Ibid.*, Part iv(A)(36).

77 *Ibid.*, Part iv(A)(32).

78 WP Working Document, *supra* note 50 at 7.

legal principles that effectively fill the gap.[79] Therefore, it is possible that the APEC Member economies could implement the APEC Framework and still be capable of providing appropriate redress in situations of rule violation, but, again, there is simply no guarantee that this would be the case.

### (c) Concluding Analysis

While the APEC Framework does meet some of the core *substantive* requirements (notably data quality/proportionality and data security) outlined by the Working Party, it is lacking in several key areas that, were it to be implemented as domestic legislation, mean it ought not to be considered "adequate" within the meaning of Article 25. The major flaw to the substantive content provisions is a series of overbroad or ill-advised exemptions. The Working Party requires that exemptions to the requirements of the core principles be limited in nature, such as those that deal with national security or public policy concerns. In contrast, the APEC Framework creates exemptions in a broader array of circumstances, reflecting its generally market-driven approach.

With regard to the Working Party's core *procedural* requirements, the APEC Framework fares even worse. There is no requirement for incorporation of any of its substantive Principles directly into the laws of APEC Member economies. Even if one were to proceed under a hypothetical scenario of the entire Framework being implemented as domestic legislation, there is still no requirement for an independent data authority, nor is there a requirement for an institutional system of adjudication in order to allow individuals to exercise their rights. While, in theory, an APEC Member economy could implement the APEC Framework and "upgrade" the provisions to meet the adequacy standard through the creation of additional rules and procedures, that potential is not enough for the APEC Framework or any legislation modeled upon it to, standing alone, be considered "adequate" by any stretch of the imagination.

The lack of procedural guarantees and relatively weak substantive provisions in the APEC Framework is consistent with its general approach to informational privacy — the APEC Framework treats it as a useful regulatory tool for consumers in a market environment, one that can be beneficial in economic terms by increasing consumer confidence. As such, any privacy rules rights are to be balanced against the economic benefits of the free-flow of that personal information. If the calculation, by an APEC Member economy, is that robust privacy regulation has adverse consequences for business, we are unlikely to see the adoption of any sort of "adequate" data protection regime. This market-oriented approach helps explain why the APEC Framework has been described as "the weakest international privacy standard yet developed."[80] According to its own guidelines for implementation, the basic concept behind the APEC Framework's principles is that "economies [have an interest] in maximising the economic and social benefits available to their citizens and businesses." The APEC Framework thereby eschews the language of rights in favour of the language of markets, placing informational privacy

79 WP Opinion on Argentina, *supra* note 61 at 13–16.

80 Graham Greenleaf, "APEC Privacy Framework Completed: No Threat to Privacy Standard" (2006) 11 Privacy Law and Policy Reporter 5 at 7.

and the benefits of cross-border data flows on an equal conceptual level.[81] In contrast, the Directive approaches the issue from a rights-based "privacy first" perspective — the Preamble states that "data-processing systems are designed to serve man" and "the object of the national laws on the processing of personal data is to protect fundamental rights and freedoms, notably the right to privacy."[82]

The APEC Framework is indeterminate and non-prescriptive, probably out of political necessity since APEC "has no treaty obligations required of its participants . . . and [its] commitments are undertaken on a voluntary basis."[83] Interpretation across Member economies that do eventually implement the APEC Framework into their domestic legislation will likely differ greatly. Indeed, this is what happened following the adoption of the OECD Principles in 1981; the general wording of the principles (strikingly similar to the APEC Framework, in fact) led to differing interpretations, thus, largely defeating the idea of creating an international document in the first place. The US went in the direction of industry self-regulation, while Europe developed a more rigorous legislative approach. Of course, the European experience was in the context of an increasingly politically and economically integrated community, unlike APEC. As such, there is less likely to be a unified interest in creating *binding* standards across the APEC economies. Indeed, the existing differences between the protections offered by the Member economies are perhaps reflective of this. It may simply be that the APEC Framework is the best that can be done with such a diverse group of states. Even so, this is not an argument in favour of the Working Party accepting those low standards as "adequate."

The APEC Framework cannot meet the Working Party's requirement of "adequacy" within the meaning of Article 25 of the Directive even if one imagines a hypothetical scenario in which it were incorporated fully into the domestic legislation of an APEC Member economy as its data protection regime. This article's analysis demonstrates that the APEC Framework is lacking, in both substantive and procedural terms. Any data protection regime adopted by an APEC Member economy could only be considered adequate if it developed a set of privacy rules that, while possibly based on the APEC Framework, went significantly beyond its minimal requirements. Yet, in 2000, the Commission appeared to bow to economic pressures and declared as "adequate" a set of American principles that also seemed to reflect a market-driven understanding of informational privacy and lacked strong procedural guarantees. Does that experience provide an applicable lesson for proponents of the APEC Framework?

---

81 *APEC Framework*, *supra* note 3, Part iv(A)(29-30).

82 *Directive*, *supra* note 2, 2nd and 10th recitals.

83 APEC, *About APEC*, online: APEC <http://www.apec.org/apec/about_apec.html>.

## V. ANALYSIS: COULD THE APEC FRAMEWORK BE RECONCEIVED AS ANOTHER "SAFE HARBOR"?

### (a) Safe Harbor

The US Department of Commerce and the European Commission agreed in 2000 to the Safe Harbor[84] privacy principles in response to concerns that the differing approach (market-driven, relying on industrial self-regulation) taken to privacy issues in the US would result in a finding of inadequacy and a halt to transfers of data. There was tremendous pressure from corporate America on the Department of Commerce to "block the Directive,"[85] and the result was a set of principles that is generally favourable to business, but one that is, nonetheless, approved by the Commission.

The Safe Harbor approach is fundamentally different than that taken by other nations wishing to meet the adequacy requirement. Canada and Argentina, for example, both developed comprehensive national legislation that matched the core principles of the Directive. In contrast, Safe Harbor does not create blanket adequacy for the US as a whole. Instead, it is a list of seven general principles, along with further explanatory details attached to the instrument as "frequently asked questions" or FAQ. Despite its name, the FAQ form as much a part of Safe Harbor as the original seven principles. American organisations can self-certify as meeting the requirements of Safe Harbor by submitting a declaration to the Department of Commerce,[86] at which point they will be considered as having guaranteed "adequate" safeguards, and can thus begin to receive and process any European data they receive. Interestingly, Safe Harbor is irrelevant to the processing of the personal data of Americans; it is strictly related to the receipt of European data flows. The thrust of the whole Safe Harbor arrangement is, therefore, entirely different than that of the European Union. The Directive requires the implementation of comprehensive national legislation that provides for robust data protections, overseen by independent data commissioners. Like the APEC Framework, Safe Harbor studiously avoids framing informational privacy as a "right"; it is an approach wary of significant government involvement in creating privacy regulations that might pose an excessive burden to business. This is, of course, consistent with the traditional market-oriented approach taken in the United States, which assumes that, in large part, industries have the ability to regulate themselves, and that "privacy" can be a value-added service like any other for which consumers can choose to pay.

### (b) The APEC Framework as another "Safe Harbor"?

This article has argued that the APEC Framework does not deserve to be accorded "adequacy" status under the Working Party's standard principles were it to be implemented as domestic legislation; but, might it be possible that an alternate route to the finding of "adequacy" could be found in a Safe Harbor-style approach?

---

84 US Department of Commerce, *Safe Harbor Privacy Principles* (2001), online: Export.gov <http://www.export.gov/safeharbor/eu/eg_main_018475.asp> [Safe Harbor].

85 Reidenberg, *supra* note 1 at 740.

86 US Department of Commerce, *Checklist for Self-Certification*, online: Export.gov <http://www.export.gov/safeharbor/eu/eg_main_018483.asp>.

In other words, could the APEC Framework be reconceived of as list of principles to which APEC-based organisations could sign up in order to receive flows of European data? Safe Harbor, after all, was the product of a series of back and forth negotiations over a period of several years.[87] This dialogue resulted in a compromise approach between the US and the EU, with the Working Party making clear its concerns as to the original proposals and the Department of Commerce responding with new proposals or modifications. The compromise seems to have centred on the WP lowering its expectations for the substantive principles in exchange for stronger procedural guarantees. For example, the creation of the FAQs, which greatly clarify how Safe Harbor is to operate in practice, was entirely the result of institutional dialogue across the Atlantic — they were nowhere to be found in the original proposals, but grew steadily in detail and in number after first being introduced. The FAQs now are considered to be on par with the Principles as part of the provisions of Safe Harbor.

The US legislative approach (or lack thereof) to the protection of personal privacy, with regard to personal data, never would have been approved by the Working Party, but the economic importance of transnational data flows to both sides led to a keen interest in a compromise. Both the Safe Harbor agreement and the APEC Framework seem to place trust in the ability of industry to self-regulate in the interests of consumer privacy, and both trace their core principles to the OECD Privacy Guidelines of the early 1980s. It might, therefore, be possible for negotiations between the EU and APEC to be opened with the hopes of reaching a similar type of compromise.

Reworking the APEC Framework to look more like Safe Harbor would require some significant changes. At this point, the APEC Framework is set up to create minimum thresholds that Member economies are encouraged to implement domestically through national legislation. In contrast, Safe Harbor is not composed of a national set of laws that apply to all entities processing information in the US, but rather a list of principles to which organisations can voluntarily subscribe, *specifically* to receive European data. If the APEC Framework were reworked in this way, it could potentially be an effective way of encouraging the adoption of better privacy standards amongst the larger corporations operating in the region, who currently have no obligation to follow the principles of the APEC Framework unless their domestic governments legislate them to do so. The encouragement would be in the form of relatively easy access to valuable European data flows, upon certification. An increased flow of information (adequately protected, of course) between Europe and Asia is certainly a positive outcome, in economic terms.

So, negotiations might conceivably lead to tighter substantive provisions and a focus on organisations rather than Member economies. However, this still leaves unconsidered the greatest weakness in the APEC Framework — an almost complete lack of effective or detailed procedural mechanisms that ensure individuals

87 See e.g. European Commission (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), *Working document on the current state of play of the ongoing discussions between the European Commission and the United States Government concerning the "International Safe Harbor Principles"* (1999) 5075/99/EN/final, online: European Commission <http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/1999/wp23_en.pdf>.

can enforce their rights. Under Safe Harbor, organisations have to explicitly agree, as part of the certification process, to accept the enforcement jurisdiction of the FTC if they fail to live up to their privacy obligations. The challenge here would be to ensure that each APEC Member economy had an institution that is as effective and as capable as the FTC in enforcing these rights. Naturally, this is more of a challenge in some states than others, depending on their level of development but, in any event, building this sort of institutional capacity is something that is difficult to achieve through negotiation alone. Furthermore, it is unclear whether some of the APEC Members with a less robust history of democracy might be convinced to create an institutional framework to enforce privacy rights of citizens even as against corporations. States that tend towards a more authoritarian governing style may also be concerned about any potential knock-on effect of acknowledging a right to privacy, regardless of the context in which it is originally granted.

While the APEC Framework is still a significant distance from the Working Party's core principles, it is important to remember that it is the Commission that makes the final recommendation as to "adequacy" status. Indeed, even in its final report to the Commission on Safe Harbor, the Working Party expressed reservations about whether the updated principles and FAQs truly met the requirements of the Directive.[88] At the same time, there was tremendous pressure on the Commission to approve the Safe Harbor agreement, both from European businesses and from some European member states themselves, who, at that time (2000), had not implemented the Directive themselves, still being in the three-year grace period.[89] It is possible, then, that the Commission could face similar pressure to negotiate with APEC to create a new approach similar to that of Safe Harbor, and it is equally possible that these negotiations could lead to improvements in some areas in which that Framework is inadequate, and to compromises in others.

### (c) Criticisms of a "Safe Harbor" Approach

While the idea of an APEC Framework reworked along the lines of Safe Harbor might seem attractive in some ways, it ought to be rejected on two grounds. First, the concept of such a self-certifying regime has proven ineffective in practice. Second, and perhaps more serious, agreeing to another "Safe Harbor"-style agreement for economic reasons threatens to weaken the normative core of the Directive and the potential it has as a global trigger for the spread of strong data privacy rights.

Five years after the issuance of the Safe Harbor principles, they had achieved limited relevance in the US. By 2005, less than 800 American corporations had signed up, less than 10% of these were in the "Fortune 500," and not a single en-

88 European Commission (Working Party on the Protection of Individuals with Regard to the Processing of Personal Data), *Opinion 4/2000 on the level of protection provided by the "Safe Harbor Principles"* (2000) CA07/434/00/EN [WP Opinion on Safe Harbor].

89 Gregory Shaffer, "Globalization and Social Protection: The Impact of the EU and International Rules in Ratcheting Up of U.S. Privacy Standards" (2000) 25 Yale J. Int'l L. 1 at 44-45, cited in Reidenberg, *supra* note 1.

forcement action had been taken against a Safe Harbor member.[90] The Commission itself has declared the slow uptake of Safe Harbor to be "a cause of disappointment."[91] Worse still, even when dealing with organisations that have subscribed to Safe Harbor, individuals may still be putting their personal information at risk. Safe Harbor tasks multiple "seal organisations" with dispute resolution, and yet only one of these proposes direct remedies to victims of privacy breaches. This is unlikely to change so long as the membership lists of those in the industry overseeing dispute resolution continue to "look like a 'Who's Who' of privacy scandal-plagued companies."[92] In its own report evaluating the effectiveness of Safe Harbor four years after its implementation, the Commission found that "a relevant number" of self-certified companies had difficulties in putting the principles of Safe Harbor into practice, particularly in the areas of notice, choice, access, and enforcement, and so recommended that the FTC be more proactive in monitoring compliance.[93] Industry self-regulation in the area of privacy seems to have failed comprehensively, suggesting that an enforceable rights-based approach, like that of the Directive, is the better strategy.

Of greater concern is that if another Safe Harbor-style approach contained the same substantive and procedural weaknesses as the original, it might threaten the normative core of the Directive and its ability to trigger stronger protections globally through the operation of Article 25. The onward transfer provision of Article 25 has helped encourage the development of more robust data protection regimes in several countries, including Canada, Argentina, and Switzerland. Perhaps the Working Party recognised the threat that Safe Harbor represented to this process when it encouraged the Commission to "bear in mind the consequences of any adequacy finding [of Safe Harbor] for future negotiations in international forums."[94] The Commission itself is also apparently conscious of this, and was careful to note in its decision finally approving Safe Harbor that it did not constitute any sort of legal precedent for findings of adequacy.[95]

Yet, it is hard to ignore the practical principle that came from finding Safe Harbor "adequate" — that where sufficient economic clout is present, the Com-

---

90 Jay Cline, "Roadmap for International Safe Harbor Framework" (2006) 20:3 Int'l. Rev. L. Comp. & Tech 361 at 362.

91 European Commission, *The Implementation of Commission Decision 520/2000/EC on the adequate protection of personal data provided by the Safe Harbor privacy principles and related Frequently Asked Questions issued by the US Department of Commerce* (2004) SEC (2004) 1323 at 5, online: European Commission <http://ec.europa.eu/justice_home/fsj/privacy/docs/adequacy/sec-2004-1323_en.pdf> [Implementation of Commission Decision].

92 Reidenberg, *supra* note 1 at 745.

93 Implementation of Commission Decision, *supra* note 91 at 7–13.

94 WP Opinion on Safe Harbor, *supra* note 88 at 2.

95 European Commission, *Commission Decision of 26 July 2000 pursuant to Directive 95/46/C of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbor privacy principles and related Frequently Asked Questions issued by the US Department of Commerce* 2000/520/EC, Article 2, online: European Commission <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32000D0520:EN:HTML>

mission will look for "acceptability" rather than "adequacy." The very purpose of Article 25 is to ensure that personal information of residents of the EU remains protected even when it is transferred beyond the borders of the Union. Watering "adequate" down to something like "acceptable" in certain cases undermines the protection Article 25 was intended to ensure, and sends the wrong message to organisations and States seeking to work with European data. Encouraging APEC to modify the APEC Framework in order to convert it to something resembling Safe Harbor would continue to send the wrong message, and would likely make it increasingly difficult for the EU to encourage widespread adoption of robust data protection laws around the world through the carrot and stick combination of Article 25.

## CONCLUSION

The APEC Framework and the EU Data Protection Directive offer two different normative conceptions of informational or data privacy. The former treats it as something that can be useful in correcting market failures and increasing consumer confidence and, as such, can more readily be balanced against economic interests. In contrast, the latter sees it as a fundamental human right tied to notions of human dignity and autonomy, and so cannot easily be restricted. These differing conceptions reveal themselves in both the substantive and procedural protections (and related exemptions) each regime grants. When one views the APEC Framework through the lens of the Working Party's own approach to findings of adequacy within the meaning of Article 25 of the Directive, it is clearly lacking. Were the APEC Framework ever to be implemented (without significant modification from the structure outlined herein) as domestic data protection legislation in an APEC Member economy, the Commission ought to reject any application for "adequacy."

While APEC is not exclusively composed of developing economies, it nonetheless has the potential for enormous economic growth relative to Europe over the next twenty-five years. As APEC's economic clout increases, the Commission may again find itself pressured from interests both inside and outside the EU to reduce the protections given to transfers of personal data outside the borders of the Union; this would be unfortunate. Any idea of opening negotiations with APEC with an eye to converting the APEC Framework to something resembling Safe Harbor ought to be rejected, for it, too, would likely fail to guarantee the requisite protections of the Directive to European data.

The EU has developed some of the world's most rigorous privacy protections for personal data, and ought not to bend them purely for economic reasons. Article 25 of the Directive has directly influenced the development of more rigorous data protection standards in other nations and (given sufficient support by the European Commission) has the potential to continue to do so. It can continue to serve as a beacon for States interested both in doing business with Europe and interested in protecting the privacy of their own citizens. While Article 25 of the Directive does not require the latter, meeting its requirements in order to keep the flow of European data uninterrupted tends to, nonetheless, have that effect as democratic gov-

ernments are unlikely to choose to require greater protection for the data of foreigners rather that that of their own citizens.[96]

Accepting the APEC Privacy Framework as a model for global consensus would be unquestionably beneficial for organisations in the "business of information," but would be a step backwards for a conception of informational or data privacy as a fundamental right, and ought to, therefore, be rejected.

96 The anomalous experience of "Safe Harbor" notwithstanding.