Privacy, Security and Transborder Data Flows – Observations from Hong Kong

(Workshop 2, Monday, 20 May 2002)

by
Raymond Tang
Privacy Commissioner for Personal Data
Hong Kong SAR

at the
National Academy of Public Administration Annual Conference
"Personal Privacy in the Digital Age:
The Challenge to State and Local Governments"
19 - 21 May 2002, Hilton Crystal City
Arlington, Virginia, USA

個人資料私隱專員公署
Office of the Privacy Commissioner
for Personal Data

Table of Contents

1 Introduction

1.1 This paper seeks to lay out some of the key privacy issues relating to trans border data flows ("TBDF") and, in particular, the respective position of the European Union ("the EU"). This position is fundamentally different from the approach developed by the USA although the end goal is much the same; the protection of data in its transfer across national borders. The United States have committed to a programme that is characterised by the tradition of voluntarism, self-regulation and self-certification; the Safe Harbor Agreement. In contrast, the Europeans have legislated for privacy and invariably established a regulatory authority to police compliance with the law. As a consequence there are, in effect, two operational models of data protection engaging different approaches. Experience has shown these models to be less than compatible and therefore current efforts are being directed towards harmonising the differences under some overarching framework. This codification process would need to recognise essential differences quite simply because it is difficult to see either of the proponents readily abandoning their positions, and the traditions upon which they based. The reconciliation of respective positions warrants careful consideration by policymakers if a confrontation is to be avoided, notably in the arena of global free trade. TBDF should therefore assume an appropriate level of importance on national and international political agendas.

1.2 In looking at the issues from the perspective of Hong Kong, where the adopted approach to privacy is more closely aligned with the European model, an attempt has been made to give the flavour of the particular circumstances that may need to be taken into account in the global security vs privacy debate. This debate has assumed a new urgency since the events of 11 September 2001. Rather too often bald assertions are made that suggest that security concerns must take precedence over privacy rights and that we will have to come to live with the fact that there is, in the pursuit of greater national security, the likelihood of greater intrusion upon the privacy of the individual. On the basis of purely localised experience the paper cautions against an over reaction to security issues quite simply because those issues are not homogeneous, or not of the same intensity, in all countries. Hong Kong is a case in point. Whilst there are very important security issues to be debated and addressed in Hong Kong in the immediate wake of 11 September there are many mitigating factors which would suggest that any response should be measured. It should also seek to strike a balance between security and privacy rather than dispatch the latter wholesale. Not only would this deny the citizens of Hong Kong their hard won right to a level of respect for their privacy but it would, without doubt,

prove very unpopular with a community in which privacy rights are now well accepted and valued.

1.3 The paper concludes by summarising a range of issues that have grown out of the TBDF debate. Those issues present policymakers with a number of challenges which need to be resolved. In striving to attain a resolution it will be necessary for negotiators to subscribe to some guiding principles that will draw the parties into an agreement that overcomes the disparities of the twin models. At the moment the forum in which this initiative should be debated is by no means clear but given the nature of the problem, and its significance, it seems that an international forum would be appropriate.

1.4 It is desirable at this juncture to draw attention to the fact that the observations made in this paper are shaped by the context in which privacy has developed in Hong Kong. In turn that context has been influenced by the European model of data protection. The intention in this paper is therefore to capture the flavour of opinion in Hong Kong rather than to attribute any superiority to the position that Hong Kong has adopted towards privacy and TBDF. Naturally that position is predicated by the local and international obligations Hong Kong is under in respect of the protection of personal data. However, the inference should not be drawn that this approach is necessarily the only approach, which is not the case, or that it is in some way the more 'correct' approach. The ensuing observations have less to do with the correctness of approach and more to do with how to reconcile apparent differences. The issues emerging from any discussion of TBDF demand clear thinking and a robust and tenable agreement that is to the mutual benefit of the parties involved and the greater global community in which information exchange takes place.

2 Personal Data Privacy in Hong Kong

2.1 Hong Kong's international status as a world class city, its unrelenting commitment to export driven growth and its history as a former colony have all influenced the manner in which, over the past decade, privacy has evolved. Today, the greater proportion of Hong Kong residents (currently there are 6.8 million of them) regard privacy, more accurately personal data privacy[1], as both an inalienable human right and important component of social policy. In the 5 plus years that the Office of the Privacy

[1] The concept of privacy existed in Hong Kong well before the PCO was established in 1995 although it must be said that among local residents understanding was initially confused and confusing. Whilst aspects of the broader concept of privacy have received increased media coverage and public debate the PCO focuses its attention upon personal data privacy. Personal data includes data that directly (name) or indirectly (E-mail address) make it practicable to ascertain the identity of an individual.

Commissioner for Personal Data ("the PCO") has been in existence awareness of, and need to protect personal privacy, has reaffirmed the original rationale for establishing the Commission.

2.2 Personal data privacy is regulated in Hong Kong by the Personal Data (Privacy) Ordinance ("the PD(P)O"). The drafting of the Ordinance, which came into effect in December 1995, was influenced by the experience of the British who had a prior history of data protection, and the EU. The EU's involvement in data or information privacy has its origins in the OECD's guidelines on data protection formulated under the auspices of Justice Michael Kirby in 1980. Twenty years on those guidelines seem rather broad and imprecise but at the time they were a bold statement of intent that said something about the need to have data/information regulated by a set of principles. The OECD principles offered a framework against which nation states subsequently developed their own privacy laws. Today, all Member States of the EU either have statutes, or are developing privacy regimens that are consistent with EU directives relating to personal data protection. From a European perspective the norm has been to commit to a statutory framework that is either federally or provincially mandated.

2.3 The EU has been instrumental in shaping the data protection laws of Member States. The intention here was to try and influence the promulgation of laws in order to produce some measure of consistency. Because of its links with Britain, the drafting of Hong Kong's privacy laws was influenced by what might be termed the European approach to privacy protection. In 1994 the Law Reform Commission of Hong Kong produced a report on the reform of the law relating to the protection of personal data[2]. The main recommendation of this report was that Hong Kong draft an ordinance that would regulate the collection, use, accuracy, retention, security and access to personal data. The legislation created the labels of Data Users - any person(s) or organizations that collect and use the personal data of an individual, and Data Subjects - the individual from whom personal data is collected e.g. a customer.

2.4 The PD(P)O is a rather technical piece of legislation that runs to some 70 sections. After in excess of five years in enforcing the Ordinance there has not been much in the way of case law and precedent to guide the application of its more esoteric provisions. To that extent enforcement has largely been the product of experience rather than clear judicial ruling. The Ordinance confers on the Commissioner powers to issue an enforcement notice which is intended both to dissuade violations of the provisions and

[2] The Law Reform Commission of Hong Kong *Report on Reform of the Law Relating to the Protection of Personal Data* (Topic 27), August 1994.

to encourage compliance. If the terms of an enforcement notice are infringed then it is possible for the miscreant to be visited with criminal sanction.

2.5 In jurisdictions that observe the European approach to data and information protection the quintessential aspects of any piece of legislation are distilled in terms of a set of information or data protection principles. This approach has been adopted for the benefit of the layman and to enable regulators to communicate the substance of the law in a manner that is readily understood. The PD(P)O has given rise to six Data Protection Principles ("DPP") which are reproduced in Appendix I. These principles confer personal data protection rights upon the citizens of Hong Kong. If the PCO's volume of business is any guide then there can be little doubt that those rights are broadly understood. More importantly they are exercised with some enhusiasm[3].

3 Section 33 of the Personal Data (Privacy) Ordinance

3.1 This section of the Ordinance, which has yet to be brought into effect, makes reference to TBDF. Essentially, section 33 prescribes the flow of personal data to and from Hong Kong i.e. certain conditions must be fulfilled for data to pass freely. These conditions are briefly outlined below.

3.1.1 There must be reasonable grounds for believing that the country to which personal data is to be transferred has in place a law which is substantially similar to the PD(P)O.

3.1.2 Where that is not the case data may only be transferred where the data subject gives explicit consent, given voluntarily, to the transfer of his/her personal data.

3.1.3 Alternatively, the data user should have reasonable grounds for believing that:

a) transfer is for the avoidance or mitigation of adverse action against a data subject;

[3] Around 2400 enquiries were registered with the PCO during its first year of operations. At the end of the fifth year of operations that figure had increased almost tenfold to 21,200. In accumulative terms the PCO has fielded in excess of 100,000 enquiries to date. In the same period complaints have risen from 52 in the first year to 790 in the fifth year. To date the Operations Division of the PCO have investigated in excess of 3000 bona fide complaints that have passed a prima facie screening test.

b) it is not practicable to obtain the consent in writing of the data subject to the transfer;

c) if it were practicable to obtain such consent the data subject would give it.

3.1.4 Personal data may be transferred where the data concerned is exempt by virtue of one of the exemption clauses contained in the provisions of the Ordinance e.g. the detection and prevention of crime.

3.1.5 Finally, the data may be transferred if the data user has taken *all reasonable precautions* to ensure that the data will not, in an overseas country be collected, held, processed or used in any manner which, if that place were Hong Kong, would be a contravention of the a requirement of the PD(P)O.

3.2 Under section 33 of the PD(P)O, where the Commissioner has reasonable grounds for believing that there is in force in a place outside of Hong Kong any law which is substantially similar to, or serves the same purpose as the Ordinance, he may by notice in the government's Gazette, specify the place so as to facilitate TBDF. In effect this clause enables the Commissioner to determine the 'adequacy' of privacy legislation and regulatory institutions in a foreign country vis-à-vis those in existence in Hong Kong.

3.3 Although section 33 has yet to be brought into effect the law clearly intends that there must be a minimum level of comparability between the legislation enacted in Hong Kong and that in a place outside of Hong Kong if TBDF is to be deemed permissible. However, what is an increasingly apparent trend, events have rather overtaken the intention of section 33 provisions. Driven by the need to cut operating costs in the economic downturn companies have begun to site some service functions outside the jurisdiction of Hong Kong. For example, call centres, IT processing, ticketing and accounting activities have either been moved over the border to Mainland China or to countries such as India. To date this development has largely gone unchecked by the PCO because section 33 is inoperative.

4 Has Hong Kong Created a Genuine Value for Personal Data Privacy?

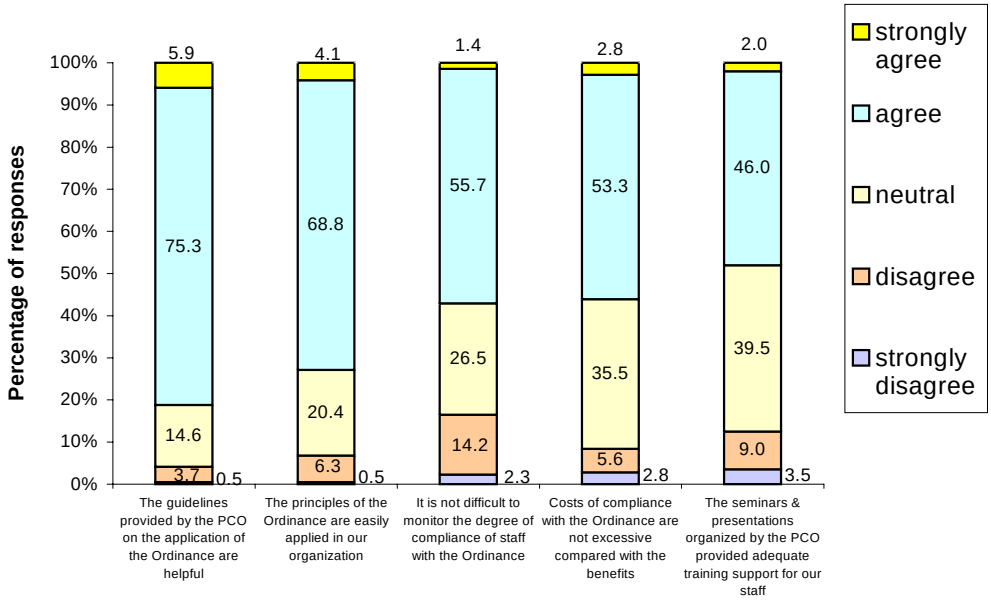
4.1 At this juncture it is as well to pause, and at least consider, this question and offer an answer. Those residing in countries where the tradition of self-regulation is often regarded as desirable, if not more than desirable than a regulatory approach, may be rather more questioning of the case being made i.e. that regulation is both needed and necessary. Is it not possible that in the process of placing a legal overlay upon privacy that governments are effectively institutionalising and bureaucratising the commodity? If that is accepted, then doesn't the whole process subject data users to needless compliance measures and associated costs that offer little in the way of value to organisations? These questions reflect perfectly normal doubts but they do not reflect the experience of the PCO in Hong Kong. How can the assertion that compliance with the provisions of PD(P)O affords business opportunities and adds value to the business be substantiated?

4.2 In Hong Kong grounds for a more positive reading of the benefits derived from a state conferred privacy regimen are to be found in the results of an annual survey of data users and data subjects commissioned by the PCO. This survey[4] is undertaken by an independent team of researchers at the University of Hong Kong. In the four years that the surveys have been conducted one of the objectives has been to measure and map the perceptions of both data users and data subjects to what the PCO would claim are the benefits to be derived from compliance with the Ordinance. Are these alleged benefits shared and if so are they of pragmatic value to data users? A couple of sets of results should serve to demonstrate that Hong Kong has not invested in an imaginary value by institutionalising privacy with public funding.

4.3 In the data users survey results for 2001 (the sample was comprised of government departments and businesses) respondents were asked to express their attitudes towards compliance. The survey results in response to that question were as follows.

[4] *The 2001 Opinion Survey of Data Users: Attitudes and Experiences* undertaken on behalf of the PCO by the Social Sciences Research Centre of the University of Hong Kong.

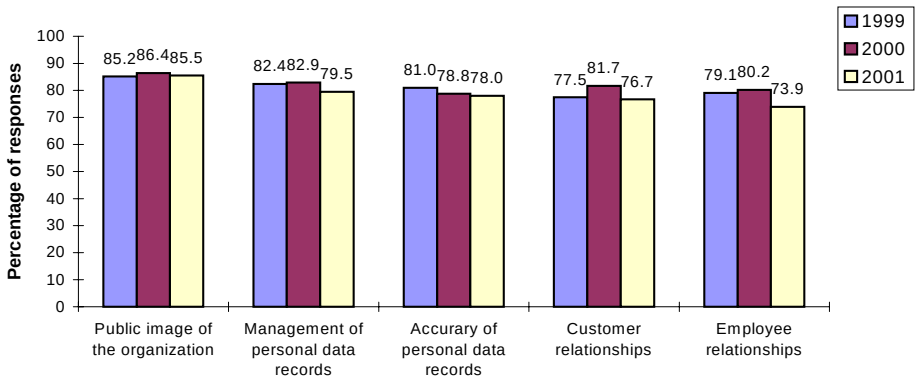
Figure 1 – The Attitudes of Data Users Towards Compliance with the Provisions of the Ordinance



The overall pattern of responses indicate a positive attitude towards compliance, which is reassuring.

Respondents were then asked to indicate to what extent they agreed with the view that compliance with the Ordinance would confer long term benefits upon the organisation. Again the results are generally encouraging, suggesting that a value is attached to compliance.

Figure 2 – The Attitudes of Data Users Towards Long Term Benefits of the Ordinance



These results, in conjunction with those derived from, previous surveys suggest that data users do *not* regard the Ordinance as an imposition; quite the contrary. Although there clearly are costs associated with compliance it is, in the Hong Kong context, at least plausible that these may more accurately be reported as an investment in good corporate governance.

4.4 Further evidence to support this view can be obtained from a study undertaken by the Law Reform Commission in 1993 in advance of the drafting of the Ordinance. The results indicate that representatives of Hong Kong business were generally in favour of the creation of a privacy regimen. This was primarily because legislation would likely comply with the EU's adequacy requirements thereby protecting the free flow of data and, by extension, business interests.

5 A Brief Comment upon Security in Hong Kong

5.1 The appalling events in New York and Washington of 11 September 2001 have irrevocably changed both government's approach to national security and citizens expectations of the measures necessary to curb international terrorism. One of the consequences of global co-operation towards the containment of terrorism has been that nation states have significantly revised their policies on data and information exchange in order to construct a more robust intelligence network. Inevitably, sweeping changes in national security arrangements will impact upon the level of privacy that individuals can legitimately expect in democratic societies around the world. In some countries, the United Kingdom for example, there is now serious political debate on the need to issue a national identity card. To have entertained that idea prior to 11 September would have been tantamount to political suicide in a country that cherishes its open and liberal democratic traditions even though it has been subject to numerous terrorist attacks over the past two decades[5].

5.2 It now appears almost inevitable that privacy advocates will have to adjust to the notion that privacy, as a human right, will have to be tempered by revised demands for national security. Whilst accepting the need to make concessions, most societies appear to want a situation in which there is a negotiated trade-off between the respective needs of national security and personal privacy. The alternative to this assumes that a significant loss of privacy will be the inevitable cost of enhanced security. However it should be possible to strike a balance between security and privacy such that they

[5] An illustration of just how liberal the United Kingdom is on the matter of the individual carrying personal identification can be gained from the fact that, because of the reporting procedures that are in place, drivers in the UK are not required to carry their driving licence on them when driving.

can co-exist. Reaching a mutually acceptable agreement will no doubt necessitate national and international debate and cooperation on the respective security and privacy issues.

5.3 It is perhaps illuminating to briefly comment upon the general mood of the public in Hong Kong in the light of the 11 September incident. On the one hand the SAR government has pledged a strong commitment to assist in the war against international terrorism. Indeed, good working relationships already exist between the Hong Kong police and other agencies of government and their counterparts in many other countries around the world. Typical areas of collaboration involve narcotics trafficking and money laundering. However, at one and the same time Hong Kong's Secretary for Security is on record as commenting that the view of the government is that Hong Kong is an unlikely target for international terrorists. This view needs to be placed in context because the impression should not be conveyed that the government of Hong Kong is in any way complacent about security issues. However, those issues are seen rather differently and have been framed by the experience of the public. In broad terms what is the nature of that experience?

5.4 As a city of world class standing Hong Kong is generally regarded as being a 'safe' city both by locals and tourists. Crimes against the person do occur but their incidence is much lower than in cities of comparable size. This of course has impacted local beliefs and behaviours in that, activities that would be perceived as being risky in some cities, appear perfectly normal to Hong Kong residents.

5.5 Since 1947 Hong Kong has had a system of identification cards which were initially issued in response to the problem of illegal immigrants. Forty five years later the HKID card system is still in place although it has been considerably upgraded over the years. More recently the government of Hong Kong have accepted an Immigration Department proposal to replace the current ID card with a smart ID card . The smart card will have a chip embedded in it along with a biometric identifier that will make if extremely difficult to forge. It will also be very difficult to assume the identity of another person. The smart card is primarily issued for the purposes of verifying the identity of the individual although it will be offered with a number of optional ancillary functions. For example, the individual may *elect* to place driver licence and library borrower details on the smart card thereby affording it added value.

In the Hong Kong context the ID card is accepted as part of everyday life rather than intrusion upon the privacy of the individual It has utility beyond verifying the identity of the individual for security needs and is indicative of the balance that can be struck between security and privacy.

5.6 In terms of airport security Hong Kong boasts one of the most sophisticated baggage and passenger security systems of any international airport. Baggage screening equipment utilises cutting edge technology, there is extensive use of surveillance cameras, the airport has it's own police division as well as an elite squad of officers trained in counter-terrorism techniques. In addition, one of the leading airlines headquartered at the airport is already evaluating radio tagging of baggage, and onboard overt and covert cameras that play on screen in the cockpit etc.

5.7 These sorts of considerations, and others, have led the citizens of Hong Kong to believe that security is adequately taken care of. To that extent the view is that the government has done well to reach a situation where security and privacy assume their respective values alongside one another. The present feeling is that Hong Kong has got the balance about right. There is no compromise on security yet in the process of attaining heightened security goals the privacy rights of the individual have remained undiluted.

It is for the reasons briefly outlined above that the people of Hong Kong see security and privacy in perhaps a slightly different light; one of complementary but different social policy issues that can, and do, coexist.

6 TBDF and European Union Directive 95/46/EC

6.1 Given Hong Kong's alignment with the European approach to privacy it is likely that, at the appropriate point in time, an application will be made to EU Commisioners to seek 'adequacy' under the provisions of the directive issued by the European parliament. Those provisions provide for the protection of individuals with regard to the processing of personal data and on the movement of such data across national borders[6].

6.2 More explicitly Chapter IV of the directive requires the existence of an adequate level of personal data protection to be in place in a third country before data can be transferred to that country from one of the EU's member countries. This requirement is frequently abbreviated to the 'adequacy' provision' and it is that concept that has become the essential feature of the EU's policy on TBDF.

6.3 The Directive goes on to make the following statements.

[6] Directive 95/46/EC of the European parliament, *The Protection of individuals with regard to the processing of personal data and on the free movement of such data*, 24 October 1995.

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

6.3.2 The Member States and the Commission shall inform each other of the cases where they consider that a third country does *not* ensure an adequate level of protection within the meaning of paragraph 6.3.1.

6.3.3 Where the Commission finds, under the procedure provided for in Article 31(2)[7], that a third country does *not* ensure an adequate level of protection within the meaning of paragraph 2 of this Article, Member States shall take the measures necessary to prevent any transfer of data of the same type to the third country in question.

6.3.4 At the appropriate time, the Commission shall enter into negotiations with a view to remedying the situation resulting from the finding made pursuant to paragraph 6.3.3.

6.3.5 The Commission may find, in accordance with the procedure referred to in Article 31(2), that a third country ensures an adequate level of protection within the meaning of paragraph 6.3.1 of this Article, by reason of its domestic law or of the international commitments it has entered into, particularly upon conclusion of the negotiations referred to in paragraph 6.3.4, for the protection of the private lives and basic freedoms and rights of individuals.

6.4 The intention of this EU directive is clear. It puts in place a mechanism that seeks to ensure that the EU, acting in concert with Member States through legislative means, regulates TBDF. In so doing the EU is seen to be upholding the rights of the individual and reinforcing fundamental data protection principles that have already been enshrined in national legislation. It is this legislative approach that has brought TBDF into sharp focus primarily because it is at variance with the free-market, self-

[7] Article 31(2) of the directive makes the following statement. 'The representative of the Commission shall submit to the committee a draft of the measures to be taken. The committee shall deliver its opinion on the draft within a time limit which the chairman may lay down according to the urgency of the matter. The opinion shall be delivered by the majority laid down in Article 148 (20) of the Treaty. The votes of the representatives of the Member States within the committee shall be weighed in the manner set out in the Article.'

regulatory approach that the US has adopted. This variance has not been without it problems. As early as 1994, if not before, the respective European and US positions appeared to be on a collision course e.g. the Citibank and German National Railway co-branded credit card[8].

6.5 In an attempt to head this problem off the US Federal Trade Commission and the EU brokered a deal called Safe Harbor. The very existence of this arrangement underscores the principled difference in approaches towards privacy on either side of the Atlantic. Safe Harbor also effectively killed off the idea that the EU directive would, by default, become the global privacy standard. This prospect had come into view as countries such as Canada, New Zealand and Australia began to align themselves with the European approach. However, that prospect was never realised and the consequence is a dual arrangement that has it roots in different value systems. This duality has given rise, on the part of the EU, to what amounts to an expression of doubt about the efficiency and efficacy of Safe Harbor. Those doubts surfaced most recently when EU commissioners reviewed the workings of Safe Harbor and published a paper on their findings. Before commenting upon that review it is as well to briefly overview the nature of this agreement struck between the USA and the EU.

7 Safe Harbor: A Self-regulatory Approach to TBDF

7.1 The Safe Harbor privacy principles were issued in July 2001 by the US Department of Commerce and were an acknowledgement of the need to bring some form of harmonisation to the disparate approaches to personal data protection in the USA and Europe. In some senses the drafting of Safe Harbor was consistent with the EU's original directive in that it established a set of principles and a process for complying with the EU's adequacy requirements. As a model Safe Harbor offers a pragmatic alternative to a statutory approach. Its weakness lies not in the framework but in the fact that it has not proved popular among American businesses. At the time of writing less than two hundred companies were listed on the Department of Commerce's website as having complied with the principles of Safe Harbor.

[8] In 1994, Citibank and the German National Railway agreed to co-brand a credit card. However, because of the fundamentally different approaches towards managing personal data in the US and Europe, German data protection commissioners felt that the deal would compromise the protection of German consumers personal data. The solution provided by the commissioners to this problem required Citibank to enter into an expensive contractual arrangement that would permit German customers to access their personal data records. One observer has commented that the nine month delay in concluding the deal between Citibank and German privacy commissioners may have cost the bank anything from US$10-50 million.

7.2 The Safe Harbor agreement is framed around seven principles which are detailed as follows[9].

7.2.1 **Notice**

Organisations must notify individuals about the purposes for which they collect and use information about them. They must provide information about how individuals can contact the organisation with any enquiries or complaints, the types of third parties to which it discloses the information and the choices and means the organisation offers for limiting its use and disclosure.

7.2.2 **Choice**

Organisations must give individuals the opportunity to choose (opt out) whether their personal information will be disclosed to a third party or used for a purpose incompatible with the purpose for which it was originally collected or subsequently authorised by the individual. For sensitive information, affirmative or explicit (opt in) choice must be given if the information is to be disclosed to a third party or used for a purpose other than its original purpose or the purpose authorised subsequently by the individual.

7.2.3 **Onward Transfer (Transfers to Third Parties)**

To disclose information to a third party, organisations must apply the notice and choice principles. Where an organisation wishes to transfer information to a third party that is acting as an agent, it may do so if it makes sure that the third party subscribes to the Safe Harbor principles or is subject to the Directive or another adequacy finding. As an alternative, the organisation can enter into a written agreement with such third party requiring that the third party provide at least the same level of privacy protection as is required by the relevant principles.

7.2.4 **Access**

Individuals must have access to personal information about them that an organisation holds and be able to correct, amend or delete that information where it is inaccurate, except where the burden or expense of providing access would be disproportionate to the risks to the individual's privacy in the case in question, or where the rights of persons other than the individual would be violated.

7.2.5 **Security**

[9] Further details regarding Safe Harbour can be found at: http://www.exports.gov/safeharbor/sh_overview.html and
http://www.exports.gov/safeharbor/sh_workbook.html.

Organisations must take reasonable precautions to protect personal information from loss, misuse and unauthorised access, disclosure, alteration and destruction.

7.2.6 **Data Integrity**

Personal information must be relevant for the purposes for which it is to be used. An organisation should take reasonable steps to ensure that data is reliable for its intended use, accurate, complete and current.

7.2.7 **Enforcement**

In order to ensure compliance with the Safe Harbor principles, there must be:

- readily available and affordable independent recourse mechanisms so that each individual's complaints and disputes can be investigated and resolved and damages awarded where the applicable law or private sector initiative so provides;

- procedures for verifying that the commitments companies make to adhere to Safe Harbor principles have been implemented and;

- obligations to remedy problems arising out of failure to comply with the principles. Sanctions must be sufficiently rigorous to ensure compliance by the organisation. Organisations that fail to provide self certification letters will no longer appear on the list of participants and Safe Harbor benefits will no longer be assured.

7.3 The Department of Commerce maintain that Safe Harbor confers the following benefits upon US and EU firms:

- All 15 Member States of the European Union will be bound by the European Commission's finding of adequacy.
- Companies participating in Safe Harbor will be deemed adequate and data flows to those companies will continue.
- Member State requirements for prior approval of data transfers either will be waived or approval will be automatically granted.
- Claims brought by European citizens against US companies will be heard in the US subject to limited exceptions.

7.4 In embracing established data protection principles The Safe Harbor Agreement was a constructive attempt to bridge the differences between the US and EU. It would certainly be true to say that it codified the rule book, albeit it on a voluntary basis, pertaining to TBDF. It has been well supported by the US Department of Commerce who have published workbooks on the agreement and procedures to ensure organisational compliance. Nonetheless, if Safe Harbor's success is to be measured in terms of the number of US organisations that sign up, it clearly cannot be regarded as such given the level of support to date. On looking at the listing of organisations what is striking, apart from the paucity of signatories, is that very few US multi-national corporations feature on the list. This phenomenon has been explained away by the fact that corporations may well regard their existing data protection practices as at least comparable with, if not superior to, the principles contained in the Agreement. Provided claims of comparability can be independently audited, which is the real substance of all compliance procedures, the merits of Safe Harbor must be in some doubt.

7.5 Although the EU has yet to deliver a final verdict on the variety of practices adopted by US corporations to meet EU standards, the fact that the vast majority have not been persuaded by the arguments advanced by the US Department of Commerce is cause for some concern. The concern in Europe being that if the codified approach to data protection afforded by Safe Harbor lacks popular support then this will give rise to diverse practices that lack consistency of approach. A US response to TBDF characterised more by fragmentation than unity of approach is likely to be regarded with some suspicion. If those suspicions are investigated and found to be true then a worse case reading of the outcome would be that TBDF could degenerate into a trade conflict between the EU and the US.

Although the EU has certainly not indicated that it will, at this stage, 'disconnect the flow' of trans-border data the situation is unlikely to go ignored given the commitment that Europeans have made to data protection legislation and regulatory institutions over the past two decades.

7.6 Similarly the US are likely to adhere to conventional wisdom if it comes to a stand-off between free market trade and data protection. Arguments advanced to reaffirm the US position have been well articulated in a paper recently published by the Heritage Foundation[10]. In summary the main points of the paper are as follows.

7.6.1 **The free movement of consumer information across borders is a key part of a free economy and a free society**

The argument advanced here is that freedom of information and TBDF, which is a logical application of information towards a particular end, has a 'far more respectable philosophical pedigree than novel principles of "data protection." A value-laden observation and one, no doubt, that EU commissioners would contest.

7.6.2 **European consumers and businesses would also benefit from less regulation**

It is argued that the freedom to access and use information in an innovative manner is precisely what has made the USA the world's largest service economy. There is learning in this both for European businesses and consumers who could expect to benefit from greater competition in the service sector driven, in part, by freedom of access to information.

7.6.3 **The focus of privacy efforts should be on threats to privacy posed by government over-regulation**

The assertion here is that whether it be Europe or the USA governments have greater powers of access to an immense amount of data. To that extent a government may present a greater risk in terms of the inappropriate use of information. In contrast the information in corporations is often restricted to vendors, customers and employees. If misuse of information should occur then government and government agencies have a greater propensity to magnify the misuse.

[10] The Heritage Foundation – Economic Freedom Project, *Privacy as a Trade Issue: Guidelines for US Trade Negotiators*, Slvieg Singleton, March 2002, pp12-13.

7.6.4 **The facts about European data protection laws should be sought from firms and individuals doing business with the EU**

The author maintains that many of the key questions that arise from data protection laws have gone largely unanswered by the supporters of those laws e.g. costs of compliance, impact upon SME's, the assessment of credit risk etc. In short the EU needs to independently corroborate the belief that the merits of data protection laws outweigh the demerits.

7.6.5 **US trade agreements should not adopt data protection as a means of satisfying EU requirements**

This would set an unfortunate precedent for future trade disputes and for US economic relations with Canada. It should be noted that, to date, Canada has not played the 'adequacy card' in terms of Canadian data in the US.

7.6.6 **US officials should be aware of discussions of data protection in other areas of the world**

The EU approach to data protection legislation is evident in other parts of the world, notably Asia e.g. Hong Kong, Malaysia and Thailand. Will the spread of data protection regimens materially advance or restrict the United States' share of global economic growth?

7.6.7 **In the area of financial services, the privacy provisions of the Gramm-Leach-Bliley Act are more than sufficient**

Argument here hinges upon the EU's preference for an 'opt in' system over an 'opt out' system of direct marketing. However, customers may find an 'opt in' system even more intrusive and the costs associated with implementing it are significant[11].

7.7 The author concludes with the observation that "Data protection laws can be expected to operate as trade barriers. The Safe Harbor' approach has not eliminated this problem both because of restrictive European interpretations of its principles and because its principles are vague and overly regulatory. The 'model contract' approach taken so far for financial services has likewise not succeeded well because the contracts supported so far by European officials do not seem to recognise fundamental business realities."

[11] The author cites the example of US West, one of the few businesses in the United States to operate an 'opt in' system. Its experience of implementing a European-style opt-in system found it cost US$30 per customer contacted to obtain a consent and required an average of 4.8 calls to each household before the company reached an adult who could grant consent. Further views on the limits of 'opt-in' can be found at http://www.cspra.org/ (February 18,2002)

7.8 This sort of analysis of TBDF between the US and the European Union is likely to be reflected in the current US Administration's negotiating position on the development of global free trade. In the absence of the emergence of a tenable working arrangement, pending a comprehensive enquiry on how to resolve the differences, corporations both sides of the Atlantic must be apprehensive of the consequences of confrontation. If data protection issues are interpreted as a restraint upon trade then there is every possibility that those issues will be referred to the WTO for adjudication. It is difficult to interpret such a state of affairs as being anything other than counter-productive to international relations and mutual trade interests. There is consequently an urgent need to seek a mutually acceptable solution.

8 The European Union's Review of Safe Harbor

8.1 In July 2001 the European Union was supposed to complete a one year review of how well non-Member States were doing in terms of compliance with the EU Directive. The date was also significant because the publication of the review was intended to mark the end of a one year moratorium imposed by the EU on its TBDF directive. However, the review was delayed and eventually published as a Commission Staff Working Paper in February 2002. Please refer to Appendix II.

8.2 Given the regulatory nature of the European approach the review was an eagerly-awaited document for the simple reason that one of its purposes was to comment upon the way Safe Harbor was working in relation to the EU Directive. In short, was there a sufficiency of comparability for the EU to pronounce Safe Harbor 'adequate'? The short answer to that is that it appears not. There is still, in the EU's opinion, some way to go before Safe Harbour is accepted as a self-regulatory approach that is compliant with the EU Directive.

8.3 The review makes a number of general observations before commenting upon perceived shortcomings in Safe Harbor arrangements. Those observations are summarised as follows.

- All the operational features of Safe Harbor are in place.
- Few companies have signed up to the scheme. The most conspicuous absence is US multi-nationals who are known to transfer vast quantities of customer/employee data to different countries around the globe.

- Although an effective mechanism has been devised to redress grievances, and allegations of denial of privacy rights, the fact remains that very few individuals have lodged a complaint.

- The EU have approved standard contractual clauses for the transfer of data to third countries as a supplementary arrangement to Safe Harbor.

- The EU is scheduled to make a comprehensive evaluation of the workings of Safe Harbor in 2003

8.4 The findings of the working paper published by the EU are based upon a "visible compliance" study derived from the postings of those organisations that have signed up to Safe Harbor. Essentially three issues of significance have been brought to the attention of the US authorities.

8.4.1 **Statements of compliance with Safe Harbor principles and/or relevant privacy policy are not systematically visible**

To comply with Safe Harbor principles it is necessary for an organisation to publish a privacy statement to that effect. The organisation should also indicate in its self-certification of adherence to the principles where the policy statement can be viewed by the public. If an organisation does not abide by its policy statements then this is legally actionable under the deceptive acts powers invested in the Federal Trade Commission ("the FTC").

The allegation made by the EU is that a "substantial number of organisations that have self-certified do not meet the requirement" established by the FTC. This procedural omission is interpreted by the EU as amounting to a loss of transparency and clarity.

8.4.2 **Privacy policies do not systematically reflect Safe Harbor principles**

Fewer than 50% of the organisations reviewed exhibited privacy policies that encompassed all seven principles enshrined in Safe Harbor. Lack of conformity with the rubric implies that organisations are not meeting their privacy obligations. This seems more than just an oversight on the part of organisations (a) because rather too many fell into this category and (b) because the Department of Commerce's Safe Harbor Workbook is very clear on the matter.

This allegation would offer comfort to those that see Safe Harbor as detrimental to business interests. Not only are the fundamental

principles of the Agreeement not being observed, but presumably costs are being incurred by organisations in the process of self-certification, the end result of which is a system that is non-compliant.

8.4.3 **Lack of transparency about how the rules apply**

The third observation made amounts to a comment on imprecise notification procedures. For example, an individual may wish to exercise his/her rights to sensitive data under an 'opt in' arrangement. However, most organisations failed to define what sensitive data was or the procedures for opting in. Secondly, the EU commented upon how complaints made by individuals would be taken up and processed by an independent dispute resolution mechanism.

8.5 From a European perspective the EU's review of Safe Harbor has identified issues that would be regarded as breaches of the principled framework upon which the Agreement is based. In the privacy regimens of Member States of the EU notions of transparency, compliance and uniformity of application are central constructs in terms of the outcomes that the protection of data seeks to achieve. Unless those outcomes *are* actually achieved then Safe Harbor is unlikely to receive endorsement from the EU as an Agreement that bridges the twin approaches. One of the reasons for this is that the Agreement must seek, as one of its primary objectives, to build trust and confidence among the public. That faith must be established not merely on the espoused principles of Safe Harbor but in their day-to-day application. Ultimately it will be the perception of the individual data subject, rather than agencies of government in the US or Europe, that will determine the reality of Safe Harbor.

9 Security, Privacy and TBDF: Some Issues to Reflect Upon

9.1 The current debate on TBDF presents policy makers with something of a dilemma. On the one hand there is an interconnectedness between security concerns, privacy protection and TBDF. On the other, there is a disjuncture in terms of the key features of alternative approaches towards data protection. This suggests that there will be strongly held differences of opinion on the appropriate avenue to take in an attempt to systematically address the challenges. In the immediate short term therefore there is a need to reach agreement on the procedural aspects of carrying the debate forward. Procedures are key to avoiding any confrontation on TBDF because of the inherent differences of approach. Those procedures should seek to provide the opportunity to avert a situation in which privacy

protection, in relation to TBDF, degenerates into a restriction upon trade. It has been suggested that if the final review of Safe Harbor, scheduled for 2003, is uncompromising then this could prove to be a defining moment in the scenario alluded to. Clearly it is not in any nation's interests to allow privacy protection to become an impediment to free trade. However, this prospect has already been debated in public and should indicate the urgency that should be attached to an agreement on procedures to head off any 'trade crisis'.

9.2 Whilst a procedural agreement would be beneficial to the respective interests of the US and EU Member States, what is less obvious is the role that respective agencies would play. In the EU one could expect the commissioners to act with legal authority because the protection of privacy is subject to the law and regulation. However, in the USA the role of the Department of Commerce and the FTC is less than clear. This creates an additional uncertainty in that if the tradition of voluntary self-regulation is adhered to by the US then no single agency of government will be able to speak authoritatively for organizations involved in TBDF. The situation is markedly different in the EU. Firstly, there is a good deal of consistency between the data protection legislation of Member States. Secondly, directives issued by EU's commissioners are invariably binding up individual States.

9.3 If the scope of debate is broadened to include countries outside of the EU and the United States then other problems arise. At the moment there are many more countries in the world *without* data protection legislation than there are with it. If TBDF is to become an international issue then a lot has to happen. Either legislation will have to be introduced in those countries which suggests that there can be no short /medium term agreement or, something like the Safe Harbor Agreement will have to be developed by national governments and examined for adequacy. Either alternative is likely to be both laborious and resource consuming. In addition, neither takes account of a whole raft of idiosyncratic data flow issues. For example, how to get countries that have an established tradition of confidentiality and secrecy around data to give that tradition up?

9.4 If TBDF becomes an adjunct to global trade issues then the question that arises is in which forum should the debate be heard? The suggestions to date range from the World Trade Organisation to the United Nations to the establishment of an International Commission.

9.5 If the forum is to have teeth then it will have to deliberate on matters of compliance standards, auditing and enforcement. This reflects an approach that the European Union is schooled in. However, such an approach is likely to be an anathema to the United States. This is because the entire

mechanism would become a regulatory imposition the benefits of which are in contention.

9.6 The issue of standards, compliance and auditing raises an argument voiced by those who regard a legislative approach as being heavy handed. The first strand to this argument is that any such arrangements would be virtually impossible to police. This is evident from the findings of the EU's review of Safe Harbor. The Agreement has been in place since 2000 yet after two years of operational experience there are reportedly too many organisations in breach of the letter and spirit of its main principles. So, what is to be done in response to those that infringe the rulebook? Is the US Department of Commerce or the Federal Trade Commission equipped to assume a policing role?

The second strand to the argument is that even if resources were available for enforcing standards it is unlikely that they would run to being able to deal with the tens of thousands of small and medium sized enterprises that may be guilty of an infraction of the rules. It would be discriminatory to concentrate compliance upon large high profile corporations and, at the same time, largely ignore smaller ones. It could be argued that, because of resource constraints and less sophisticated operational systems smaller organisations could be the source of the greater proportion of violations. Quite simply, the larger corporation is better equipped to comply, and to focus upon them, when non-compliance is prevalent among small and medium sized firms, would be unacceptable.

9.7 However, if one piece of research is to be believed than all the talk of compliance may amount to an over-reaction. That is, infractions are genuine mistakes, relatively trivial, or regarded as not being worthy of filing a complaint with the appropriate authorities.

Recently the Cato Institute undertook a survey of European data regulation agencies. One question asked in that survey was, "Were any (and if so how many) companies fined or cited for transferring data from (the respective nation) out of Europe in the past?" The results, reproduced in Figure 3 are revealing[12].

Figure 3 – Survey of Enforcement Actions Taken under the EU Directive

Country	Response to Survey Question

[12] Cited in The Cato Institute Centre for Trade Policy Studies, *Safe Harbor or Stormy Waters? Living with the EU Data Protection Directive,* Aaron Lukas, p23

Yes = Enforcement Action Taken	
EU Commission	Refused to answer
Austria	Yes
Belgium	None known
Denmark	None known
Finland	Yes
France	No response
Germany	Yes
Greece	No response
Ireland	None known
Italy	None known
Luxembourg	Referred to the EU Commission
Netherlands	None known
Portugal	None known
Spain	No response
Sweden	None known
United Kingdom	Yes (prior to the directive)

Source: The Cato Institute

One can only speculate upon the reasons explaining the paucity of enforcement action in the EU: lack of vigilance; inadequate funding for compliance activities; individuals lack of awareness regarding their data protection rights; the nature of the infractions were minor and did not warrant a full investigation. Whatever the reason the evidence of this piece of research plays into the hands of those that regard standard setting, auditing and enforcement measures as something of a bureaucratic excess. A solution looking for a problem.

9.8 The bottom line of any comprehensive agreement for bridging the divide that exists between the EU and the United States may turn out to be a very basic one. What will compliance with any future agreement cost the organisation? If compliance is perceived by business as another operating cost, rather than as an investment in consumer goodwill, then cost arguments will feature heavily in terms of the stand taken by US corporations towards TBDF and data protection. Unless organisations like the EU, or some global alliance of privacy groups, can produce persuasive arguments to the contrary one suspects that corporate America will continue to play a waiting game before revealing its hand.

10 Concluding Comments

10.1 As pointed out earlier it seems that neither the EU nor the United States will abandon their respective positions on data protection/information flow. That decision should be accorded sovereign respect. However, it is possible to speculate upon a number of factors that could precipitate a reaction that would bring some urgency to the negotiating table.

- A comprehensive review of Safe Harbor by the EU is scheduled for 2003. In the interim it remains to be seen whether the alleged deficiencies of the Agreement are adequately redressed. This means that signatories will have to incorporate the seven principles and consistently apply them to their data protection policies. If the 2003 review comes to the conclusion that Safe Harbor is not working as intended then the US will feel the need to offer some form of explanation. Whether that explanation will be accepted by the EU, or whether it means that Safe Harbor has fallen short of providing a level of compatibility sought by the Europeans, remains to be seen.

- Ultimately it is trade issues that will lead to an intensification of the debate. If legal cases in Europe allege a violation of the individual's privacy rights and if the judgement is in favour of the plaintiff then the EU will be obligated to confront the USA with the verdict. If that verdict were to disrupt TBDF and jeopardise trading relationships, then there is going, in the relatively near future, to be a destabilisation of trans Atlantic trade. This cannot be anything other than to the detriment of national, trade and consumer interests.

- What type of activity might precipitate a degeneration of the current situation between the US and EU? A civil action is one possibility, but practices such as data mining and website tracking could provide the conditions that would harden the resolve of the parties. For example, the information brokerage business involves intermediaries who extract personal data from websites and use this to compile lists that reflect a particular consumer profile. These lists are then sold to third parties around the world for use in direct marketing campaigns. If this type of evidence were to be presented to the EU by a privacy pressure group, or academic research institute, the EU would find it difficult to ignore the findings. If the findings were then independently verified it would be equally improbable that the EU would take no action.

- If the threat outlined above looks increasingly like a reality then there is a good case for arguing that insofar as TBDF are concerned there should be movement towards a global privacy standard that would avert any interruption in trade. It may originally have been thought that the EU were pioneering this avenue but given the US

position some other compromise will have to be found by policymakers.

- How should policy makers proceed as the EU Directive / Safe Harbor saga plays out? A useful place to start would be to look at model arrangements that have been authored to facilitate a reciprocal exchange of information between countries. Given the essential difference in the approach to data protection in Canada and the US it might be fruitful to look at TBDF in microcosm and regard this example as a case study from which more generalisable principles can be forged. Alternatively, existing bi-lateral or multi-lateral information sharing agreements that work well may be another starting point. These agreements invariably permit the exchange of particular classes of data without massively violating the privacy rights of the individual. The sorts of arrangements that come to mind are double taxation agreements or the sharing of criminal intelligence e.g. Interpol. The manner in which these arrangements evolved may offer valuable learning for those engaged in developing data protection standards that do not violate the flow of data necessary to promote trade.

10.2 It may well be that the incentive to reach consensus on the balance between data protection and the free flow of information may come from the market. In a world environment that is increasingly dominated by global trade, both on and offline, it may be a corporation's customers that ultimately call the shots. If customers of corporations that have a global presence begin to articulate broad-based disapproval of the manner in which their personal data are used then one can expect a reaction from corporate leaders. To date there has not been an incident that has caught the attention of the world's media. However, the recent ruling against DoubleClick is indicative of practices that incur the wrath of consumers. It also indicates the possible shape of things to come in terms of the legal sanctions to be applied[13] against those corporations that either skirt the law or flout the principles underlying consumerism.

10.3 The indications are that control of personal data is of growing importance to consumers in the global E-economy. If marketers are found to violate consumers perceptions regarding the abuse of their personal data and online privacy, then the need for control will ensure an appropriate

[13] Earlier this year DoubleClick was ordered to pay US$1.8 million in costs to 31 law firms representing plaintiffs to settle federal and state class-action litigation against the company regarding its online privacy practices. Proceeding's against DoubleClick began after it acquired the direct marketing firm Abacus. After acquisition DobleClick announced plans to link Abacus's database of names and addresses with DoubleClicks' database of Internet user behaviour.

censuring of those practices. This can only be detrimental to goodwill, corporate image and the loyalty of consumers. These sorts of intangible assets are of considerable value to a corporation and it may be this that drives a new level of corporate respect for data protection such that control of personal data remains in the hands of the consumer[14]. Caveat venditor!

10.4 In conclusion, and in anticipation of a deadlock in attempts to span the divide between the EU and the US on TBDF, it would be prudent for policymakers to act in this transitional period by reflecting upon the range of options in a post-Safe Harbor world. The US commitment to a tradition of voluntary self-regulation is patently obvious. Equally, the EU's right to legislate for data protection must be accepted as inviolable. But, both the EU and US are party to international agreements on trade that should not be unfairly disadvantaged because of differences in their respective positions. If the law is taken out of the equation then policymakers may benefit from asking whether lack of regulation will have the concomitant effect of diminishing privacy. This is where the customers of global corporations need to be factored in because it is the power of the marketplace i.e. consumer preferences and spending behaviour that will probably motivate the parties to devise a consensus model.

10.5 Another factor to be considered is that data protection lends itself to a technological solution. If the customer is reassured that the application of privacy-enhancing technology ("PET") will provide adequate safeguards, and this can be demonstrated, then PET may be a powerful tool in making the customer and his/her personal data anonymous. Technology is therefore likely to be part of the mix of any formula that seeks to preserve TBDF and, at one and the same time, ensure that that control of personal data resides with the individual. One thing is for sure, arriving at that formula will require a negotiated compromise that is equitable and workable. To achieve that goal both the US and the EU will have to learn from each other and apply that learning. There is nothing to be gained from either party 'digging in' and adopting an adversarial stance.

The Office of the Privacy Commissioner for Personal Data
Unit 2001, 20th Floor, Convention Plaza
1 Harbour Road
Wanchai
Hong Kong SAR

Tel : (852) 2827 2827
Fax: (852) 2877 7026

[14] A recent articulation of the value of marketers respecting consumers need to control their personal data can be found in *Permission Marketing,* Seth Godin, Simon and Schuster, 1999.

E-mail: pco@pco.org.hk
Website: www.pco.org.hk

Appendix I
PD(P)O – Data Protection Principles

SCHEDULE 1
DATA PROTECTION PRINCIPLES

1. Principle 1 - Purpose and Manner of Collection of Personal Data

(1) Personal data shall not be collected unless -
(a) the data are collected for a lawful purpose directly related to a function or activity of the data user who is to use the data;
(b) subject to paragraph (c), the collection of the data is necessary for or directly related to that purpose; and
(c) the data are adequate but not excessive in relation to that purpose.

(2) Personal data shall be collected by means which are
(a) lawful; and
(b) fair in the circumstances of the case.

(3) Where the person from whom personal data are or are to be collected is the data subject all practicable steps shall be taken to ensure that
(a) he is explicitly or implicitly informed, on or before collecting the data, of -
(i) whether it is obligatory or voluntary for him to supply the data; and
(ii)where it is obligatory for him to supply the data, the consequences for him if he fails to supply the data; and
(b) he is explicitly informed -
(i) on or before collecting the data, of -
(A) the purpose (in general or specific terms) for which the data are to be used; and
(B) the classes of persons to whom the data may be transferred; and

(ii) on or before first use of the data for the purpose for which they were collected, of -
(A) his rights to request access to and to request the correction of the data, and
(B) the name and address of the individual to whom any such request may be made,

unless to comply with the provisions of this subsection would be likely to prejudice the purpose for which the data were collected and that purpose is specified in Part VIII of this Ordinance as a purpose in relation to which personal data are exempt from the provisions of data protection principle 6.

2. Principle 2 - Accuracy and Duration of Retention of Personal Data

(1) All practicable steps shall be taken to ensure that -
(a) personal data are accurate having regard to the purpose (including any directly related purpose) for which the personal data are or are to be used

(b) where there are reasonable grounds for believing that personal data are inaccurate having regard to the purpose (including any directly related

purpose) for which the data are or are to be used -

(i) the data are not used for that purpose unless and until those grounds cease to be applicable to the data, whether by the rectification of the data or otherwise, or

(ii) the data are erased

(c) where it is practicable in all the circumstances of the case to know that -

(i) personal data disclosed on or after the appointed day to a third party are materially inaccurate having regard to the purpose (including any directly related purpose) for which the data are or are to be used by the third party, and

(ii) that data were inaccurate at the time of such disclosure, that the third party-

(A) is informed that the data are inaccurate and

(B) is provided with such particulars as will enable the third party to rectify the data having regard to that purpose.

(2) Personal data shall not be kept longer than is necessary for the fulfillment of the purpose (including any directly related purpose) for which the data are or are to be used.

3. Principle 3 - Use of Personal Data

Personal data shall not, without the prescribed consent of the data subject, be used for any purpose other than -

(a) the purpose for which the data were to be used at the time of the collection of the data, or

(b) a purpose directly related to the purpose referred to in paragraph (a).

4. Principle 4 - Security of Personal Data

All practicable steps shall be taken to ensure that personal data (including data in a form in which access to or processing of the data is not practicable) held by a data user are protected against unauthorized or accidental access, processing, erasure or other use having particular regard to -

(a) the kind of data and the harm that could result if any of those things should occur;

(b) the physical location where the data are stored;

(c) any security measures incorporated (whether by automated means or otherwise) into any equipment in which the data are stored;

(d) any measures taken for ensuring the integrity, prudence and competence of persons having access to the data, and

(e) any measures taken for ensuring the secure transmission of the data.

5. Principle 5 – Information to be Generally Available

All practicable steps shall be taken to ensure that a person can –

(a) ascertain a data user's policies and practices in relation to personal data;

(b) be informed of the kind of personal data held by a data user;
(c) be informed of the main purposes for which personal data held by a data user are or are to be used.

6. Principle 6 - Access to Personal Data

A data subject shall be entitled to -

(a) ascertain whether a data user holds personal data of which he is the data subject;
(b) request access to personal data -
(i) within a reasonable time;
(ii) at a fee, if any, that is not excessive;
(iii) in a reasonable manner and
(iv) in a form that is intelligible;
(c) be given reasons if a request referred to in paragraph (b) is refused;
(d) object to a refusal referred to in paragraph (c);
(e) request the correction of personal data;
(f) be given reasons if a request referred to in paragraph (e) is refused; and
(g) object to a refusal referred to in paragraph (f).

Appendix II
EU Commission Staff Working Paper on the Adequacy of Safe Habor Privacy Principles

COMMISSION OF THE EUROPEAN COMMUNITIES

Brussels, 13.02.2002
SEC(2002) 196

COMMISSION STAFF WORKING PAPER

The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce

COMMISSION STAFF WORKING PAPER

The application of Commission Decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequate protection of personal data provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce

Executive summary

On 26 July 2000, the Commission adopted Decision 520/2000/EC recognising the Safe Harbour international privacy principles, issued by the US Department of Commerce, as providing adequate protection for the purposes of personal data transfers from the EU.

The Parliament's resolution of 5 July 2000 called on the Commission to ensure that the operation of the Safe Harbour was closely monitored and to make periodic reports. In remarks to the Parliament's Committee for Citizens Rights and Freedoms, Commissioner Bolkestein said that the Commission would prepare such a report before the end of 2001. The present working document responds to that undertaking.

On the basis of the information collected from the US Department of Commerce's web site, where organisations adhering to the Safe Harbour and information about them are listed; from US public authorities and private sector organisations involved in dispute resolution and enforcing Safe Harbour commitments; from the EU Member States' data protection authorities (DPAs) which also play a role in enforcing Safe Harbour commitments and from the web sites of the organisations that had adhered to the Safe Harbour by 4 June, the Commission's services note that:

- All the elements of the Safe Harbour arrangement are in place. The framework is providing a simplifying effect for those exporting personal data to the 129 US organisations in the Safe Harbour as of 1 December 2001 and reduces uncertainty for US organisations interested in importing data from the EU by identifying a standard that corresponds to the adequate protection required by the Directive.

- Individuals are able to lodge complaints if they believe their rights are been denied, but few have done so and to the Commission's knowledge, no complaint so far remains unresolved.

- A substantial number of organisations that have self-certified adherence to the Safe Harbour do not seem to be observing the expected degree of transparency as regards their overall commitment or as regards the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard..

- A wide array of sanctions to enforce Safe Harbour rules exist under dispute resolution mechanisms. But not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbour rules and not all

have in place privacy practices applicable to themselves that are in conformity with the Principles, as required by Safe Harbour rules. Enforcement is a key element in the Safe Harbour framework and it is therefore necessary that Safe Harbour organisations use only dispute resolution mechanisms that fully conform to Safe Harbour requirements.

The Commission's recent Decisions approving standard contractual clauses for the transfer of data to third countries in no way affect the validity of the Safe Harbour arrangement, which should remain an attractive option for eligible organisations regularly involved in data transfers. The Commission services will continue to co-operate with the Department of Commerce in encouraging US organisations to join and to insist on a rigorous respect for the transparency requirements of the Safe Harbour. The Commission's services and the US Department of Commerce have agreed that transparency is a vital feature in self-regulatory systems and they look to the organisations concerned to improve their practices in this regard. They consider that some at least of the shortcomings identified can be put down to "teething problems". The Commission's services welcome the readiness of the US Department of Commerce to address some of them through improvements in the self-certification process. They consider that it is through the vigilance and enforcement action of the relevant public authorities in the US that the arrangement will remain credible and serve its purpose as a guarantee of adequate protection for personal data transferred from the EU to the US.

Other stakeholders including consumers and business may find this working document useful in order to make their own assessment of the application of the "Safe Harbor" arrangement. We would welcome such assessments which would also be a useful contribution to the Commission's evaluation of the Safe Harbor arrangement planned for 2003.

Introduction

Exercising the powers conferred on it by Article 25(6) of Directive 95/46/EC, the Commission adopted on 26 July 2000, Decision 520/2000/EC[1] recognising the Safe Harbour international privacy principles, issued by the US Department of Commerce, as providing adequate protection for the purposes of personal data transfers from the EU. This Decision was subject to prior scrutiny by the European Parliament, in accordance with Council Decision 1999/468. The Parliament's resolution, adopted on 5 July 2000, called on the Commission "to ensure that the operation of the safe harbour system is closely monitored.... and to make periodic reports to the working party provided for in Article 29 and the Committee provided for in Article 31 of Directive 95/46/EC, as well as to the relevant committee of the European Parliament." In remarks to the Parliament's Committee for Citizens Rights and Freedoms, Commissioner Bolkestein said that the Commission would prepare such a report before the end of 2001. The present Commission services working document responds to that undertaking.

The Commission's Decision requires the Commission to make an evaluation of the Decision's implementation after 3 years[2]. This working document does not replace or anticipate that evaluation. Nor is it intended to substitute the role of any of the enforcement bodies involved in the Safe Harbour arrangement, or the process of verification provided for in Frequently Asked Question 7 in the FAQs issued with the Safe Harbour principles.

The Commission has collected information from the Department of Commerce's web site, where organisations that have self-certified their adherence to the Safe Harbour and information about them are listed; from US public authorities and private sector organisations involved in dispute resolution and enforcing Safe Harbour commitments; from the EU Member States' data protection authorities (DPAs) which also play a role in enforcing Safe Harbour commitments and from the web sites of the organisations that self-certified by 4 June. Its objectives were:

(a) To gather information on all the elements of the Safe Harbour framework and whether they have been put in place, both in the US and in the EU and are having the desired effects for those involved in data transfers.

(b) To ascertain whether complaints by individuals about alleged breaches of Safe Harbour obligations have reached dispute resolution or enforcement bodies and if so, whether they have been satisfactorily resolved.

---

[1] Commission decision 520/2000/EC of 26 July 2000 pursuant to Directive 95/46 of the European Parliament and of the Council on the adequacy of the protection provided by the Safe Harbour Privacy Principles and related Frequently Asked Questions issued by the US Department of Commerce in OJ 215 of 28 August 2000, page 7

[2] Article 4<<1. This Decision may be adapted at any time in the light of experience with its implementation and/or if the level of protection provided by the Principles and the FAQs is overtaken by the requirements of US legislation.
2. The Commission shall in any case evaluate the implementation...on the basis of available information three years after its notification...and report the findings to the Committee...including any evidence that could affect the evaluation that the provisions set out in Article 1...provide adequate protection...and any evidence that the present Decision is being implemented in a discriminatory way.
3. The Commission shall, if necessary present draft measures in accordance with the procedure referred to in Article 31 of Directive 95/46>>.

(c) To see whether "visible" material provided on their web sites by organisations that have self-certified their adherence to the Safe Harbour is in conformity with their Safe Harbour obligations.

(d) To see whether, judging by their web sites and other material provided by them, the US alternative dispute resolution bodies selected by organisations adhering to the Safe Harbour complied with the requirements for such bodies set out in the Enforcement Principle and FAQ 11.

(a) Are all the elements of the Safe Harbour in place?

On the US side

On 29 September 2000 the US Department of Commerce published a notice in the Federal Register laying down procedural steps that companies needed to take in order to register in the list of adherents to the Safe Harbour. These conformed with the requirements laid down in FAQ 6 on self-certification.

The Safe Harbour has been operational since 1st November 2000 when the US Department of Commerce opened the on-line self-certification process for US organisations wishing to adhere to the Safe Harbour Principles. As of 1 December 2001, there are 129 US based organisations that have self-certified their adherence to the Safe Harbour Principles and are listed in the public list kept by the US Department of Commerce (http://www.export.gov/safeHarbor/).

The number of companies to have self-certified and that can therefore be assured of the benefits of the Safe Harbour is lower than expected, but this does not seem to have affected the effectiveness of the arrangement. Companies that choose not to join have to provide adequate safeguards in other ways, for example through contracts. It is expected that Safe Harbour membership will continue to grow steadily, now that the Safe Harbour has got off to a relatively trouble-free start.

The US Department of Commerce has undertaken several initiatives to inform companies about the Safe Harbour and to encourage them to join. The DoC web site contains extensive material on the rules that have to be followed by organisations. Its education and outreach plan has included the development an implementation manual, "the Safe Harbour Workbook"[3] and a series of seminars held in major US cities. Moreover, staff of the Office of Electronic Commerce routinely answer company inquiries concerning Safe Harbour and provide immediate follow-up to these inquiries. A continued effort to explain Safe Harbour rules through workshops, web casts and round table discussions is foreseen for next year.

On the EU side

Member States were obliged to put in place any necessary provisions to allow for data to flow to US organisations in the Safe Harbour list by 25 October 2000, that is ninety days after notification of the decision. In most Member States there was no need to change existing provisions. In Sweden, the Decision was transposed on 1 January 2001 through a change in the Personal Data Ordinance (1998:1191), section 12/13. On 24 November 2000, the Finnish Personal data protection Act 986/2000 was amended to allow for all Commission decisions based on Article 25.6 of the Directive to have the force of law. In

[3] available at http://www.export.gov/safeHarbor/sh_workbook.html

Belgium, a Royal Decree on cross-border data flows is expected to be adopted in the coming months. Until then Commission decision 520/2000/EC has direct effect in Belgium. In Ireland, pending publication of the bill transposing directive 95/46, Articles 25 and 26 of the Directive will be given statutory effect by way of Regulations presently being finalised. In other cases, the implementation of the Commission's decision recognising the adequacy of the Safe Harbour is carried out by the national data protection Commissioner. Such is the case for Italy[4].

There was also a requirement to set up and make operational the panel of EU data protection authorities (DPAs: "the Panel") referred to in FAQ 5 for those adherents to the Safe Harbour which opt to co-operate with DPAs rather than to nominate alternative dispute resolution bodies in the US. This option, initially available for three years, is compulsory when human resources data are transferred from Europe to a Safe Harbour organisation (FAQ 9). FAQs 5 and 9 lay down the general framework for this co-operation. The internal operating procedures for the Panel were agreed by the Article 29 Working Party in November 2000 and are posted on the panel's web site: (http://forum.europa.eu.int/Public/irc/secureida/safeHarbor/home). Participation in the work of the panel is open to the supervisory authorities of all Member States, but is voluntary. Contact details of the 8 DPAs that participate can be found on the web site.

As provided for in FAQ 5, US organisations have to pay an annual fee designed to cover the operating costs of the Panel. The annual fee is payable to a bank account managed by the US Council for International Business (USCIB), US affiliate of the International Chamber of Commerce, acting as a trusted third party on behalf of the Data Protection Panel. The Commission is grateful to the USCIB for agreeing to fulfil this role and to the International Chamber of Commerce for its good offices.

Further to FAQ 11, the Panel has adopted and posted a standard complaint form in all Community languages to facilitate the complaint resolution process. This form is also available on its web site as well as from the DPA in each Member State.

For their part, the Commission services have posted on the Europa web site[5] all Safe Harbour documents in all 11 Community languages, the European Parliament's resolution and the opinion of the Article 29 Working Party. It has also posted a series of questions and answers on "How will the Safe Harbour arrangement for personal data transfers to the US work". Routinely guidance on specific questions is provided either by telephone or through the Internal Market Directorate General's e-mail box[6]. On 15 June 2001, the Commission published a guide entitled "Data Protection in the European Union". The guide does not deal specifically with the Safe Harbour, focusing instead on the application of the EU Directive but it provides details of the procedure to introduce a complaint, as well as the contact details for the offices of the DPAs in each of the Member States. Nine national data

---

4 On 10 October, Italy's *Garante per la protezione dei dati personali* issued "Authorisation for the Transfer of Personal Data to Organisations Established in the United States of America in Compliance with the "Safe Harbour Privacy Principles". The Garante has reserved the right to perform the necessary controls on lawfulness and fairness of data transfers and processing operations preceding the transfers as well as on compliance with the above mentioned Principles and in pursuance of Community law and Act no. 675/1996 to take action (if necessary) by suspending or prohibiting the transfer. The authorisation is published in the Gazzetta Ufficiale of 26 November and available in the English section of the Garante's web site

5 europa.eu.int/comm/privacy

6 MARKT-A4L@cec.eu.int

protection offices in the Member States provide information through their web sites about the Safe Harbour arrangement (UK, NL,FR, DE, IRE, IT, SW, Fl and GR). None has at present a link to the Panel's web site, but the Commission services have invited the authorities concerned to make such links.

The Commission's services are not aware of any case in which difficulties have arisen for those involved in transferring personal data from the EU in connection with transfers to organisations that have adhered to the Safe Harbour.

(b) Have complaints about breaches of **Safe Harbour obligations been received and were they satisfactorily resolved?**

US companies claiming to comply with the Safe Harbour Principles and not in fact doing so may face sanctions by US enforcement mechanisms. Safe Harbour rules require that each organisation m the Safe Harbour endows itself with a readily available, affordable and independent third party dispute resolution mechanism by which individual complaints are investigated and disputes resolved by reference to the Safe Harbour Principles[7].

As of 7 December 2001, six US private sector organisations have been chosen by organisations in the Safe Harbour to operate as their dispute resolution bodies. They are BBBOnline, TRUSTe, the Direct Marketing Safe Harbour Program[8], Entertainment Software Rating Board Privacy Online EU Safe Harbour Programme, the Judicial Arbitration and Mediation Service (JAMS)[9] and the American Arbitration Association. These private sector dispute resolution bodies have attracted a total of 54 organisations in the Safe Harbour, the remaining choosing to co-operate with EU data protection authorities in accordance with FAQ 5. Information provided by the dispute resolution bodies, including the DPAS, indicates that very few complaints have been filed against organisations in the Safe Harbour and that all of them have been resolved without enforcement action being taken. Indeed, only TRUSTe so far reports having received some complaints (27) against Safe Harbour participants. It **is** not clear how many of these complaints concerned data received from the EU, as TrustE does not keep track of the origin of the complaints. The DPAs panel has so far received no complaints.

Safe Harbour commitments are enforceable under Section 5 of the Federal Trade Commission Act and (as regards organisations in the transportation sector) under Title 49 United States Code Section 41712. The Federal Trade Commission report that no cases of unresolved complaints resulting from alleged breaches of Safe Harbour rules have been brought to their attention.

---

[7] see FAQ 11

[8] The DMA Safe Harbour programme is a dispute resolution mechanism offering a free service initially open to members of the Direct Marketing Association only. Membership of the DMA does not trigger adherence to the Safe Harbour. In fact organisations have to apply separately to join the DMA Safe Harbour Programme, publish a privacy policy in conformity with the Principles and self-certify to the US Department of Commerce.

[9] The first three process complaints from online or offline data. ESRB processes complaints from data collected online but processed offline.

(c) Is "visible" material provided on their web sites by organisations that have adhered to the Safe Harbour in conformity with their Safe Harbour obligations?

As part of its preparations for this report the Commission's services commissioned a "visible compliance" study (based on what was posted on the web sites of Safe Harbour participants on 4 June) from the independent consultant currently under contract to help evaluate data protection arrangement outside the EU. The services also carried out their own information-gathering exercise through random checking gathering exercise through random checking of material made available by the organisations concerned, mostly through their web sites. Information on the application of the framework was also exchanged with dispute resolution bodies and the Member States data protection authorities. No US organisations have been audited by the Commission. The results of the information-gathering exercise have been shared with the US Department of Commerce and the Federal Trade Commission. The Commission services have drawn the attention of the Department of Commerce and the FTC to the following concerns which emerge from the examination of "visible" material provided by participants in the Safe Harbour:

=> Statement of adherence to Safe Harbour Principles and/or relevant privacy policy not systematically visible

To enjoy the benefits of the "Safe Harbour", companies must register with the US Department of Commerce and publicly declare their adherence to the Safe Harbour principles. Although there are in principle other ways of qualifying, at present all organisations listed qualify for Safe Harbour rights exclusively through self-regulatory efforts. To do so in compliance with Safe Harbour rules, it is necessary for an organisation to publish a privacy policy that is compliant with the Principles and to indicate in the organisation's self-certification of adherence to the Safe Harbour Principles where this policy can be viewed by the public. FAQ 6 requires that "All organizations that self-certify for the Safe Harbour must ... state in their relevant published privacy policy statements that they adhere to the Safe Harbour Principles". In addition, if an organisation does not abide by its stated policies this is actionable under Section 5 of the FTC Act or similar statute.

A substantial number of organisations that have self-certified do not meet the requirement in FAQ 6 quoted above. For some, no public statement of adherence to the Safe Harbour Principles could be found, apart from the self-certification itself. For a small number, the privacy policy mentioned in the self-certification could not be accessed. The Commission's services have been assured by the Department of Commerce and the Federal Trade Commission that the self-certification itself is a public declaration providing a sufficient basis on which the FTC could take enforcement action under its deceptive acts powers. The Commission's services welcome these assurances... Nevertheless, these omissions do mean that Safe Harbour participants are in some cases falling short of what the texts require, with a resulting loss of transparency and clarity, in particular *vis-a-vis* the public in general.

A specific difficulty arises in this respect in the case of transfers of employment data. Some organisations have chosen to adhere to the Safe Harbour only for the purpose of transferring employee data from the EU. Such organisations self-certify to the Department of Commerce in the usual way, but do not post a statement of adherence to the Principles or a privacy policy or specify an Internet location for such a policy for the public to see. They rather confine this to in-house arrangements such as employee manuals or intranets. This ensures that the employees who are the data subjects affected by these policies in principle have access to them. This practice is understandable but is not in strict conformity with Safe Harbour requirements. The organisations should make the policies available on request.

Moreover, it would be preferable that even privacy policies only concerning employees be immediately and directly accessible by the relevant dispute resolution bodies (in this case the DPAs, as required by FAQ 9). The present situation lacks full transparency and the Commission services will draw this matter to the attention of the DPAs.

=> *Privacy Policies do not systematically reflect Safe Harbour Principles.*

Less than half of organisations post privacy policies that reflect all seven Safe Harbour Principles. Some Safe Harbour Principles (such as the Security Principle) are mentioned by a majority of organisations, whilst others generally tend not to be mentioned (e.g. the Access Principle, including the right to amend incorrect data).

As already indicated, the Commission's services' reading of the Safe Harbour texts as a whole is that participants relying on self-regulation must have a privacy policy and that this should be in conformity with the Principles. While the Department of Commerce places more emphasis on the act of self-certification, its Workbook on the Safe Harbour recommends that organisations should cover all the Principles in their published policies. As mentioned above, no US organisation has been audited and the absence, for example, of a statement about access does not necessarily mean that access is not granted when requested. Nevertheless, the Commission services consider that if privacy policies of Safe Harbour organisations do not reflect all the principles this would be a cause for some concern. For example, the organisations concerned may not have understood and may not therefore be meeting the full range of their Safe Harbour obligations. The recommendation in the above-mentioned DoC Workbook is exemplary and approach followed by the minority of Safe Harbour organisations that have so far complied with it is to be commended.

=> *Lack of transparency about how the rules apply*

There is also in many cases a lack of clarity for individuals who might wish to exercise their rights *vis-á-vis* data about them held by an organisation in the Safe Harbour. For example, a majority (but not all) organisations state that they provide for opt-in for sensitive data, but few indicate what sensitive data is. As far as the enforcement provisions are concerned, fewer than half of participants inform individuals of the arrangements for taking up complaints with an independent dispute resolution mechanism. Whilst in some cases there is a display of the seal of dispute resolution bodies, most organisations have chosen to co-operate with the DPAs and in general they do not indicate how the DPAs can be contacted. In some cases, more than one privacy policy is posted by the same organisation and sometimes with no visible reference to adherence to the Safe Harbour. There is nothing in the Safe Harbour texts that forbids multiple privacy policies, and it is indeed understandable that some companies have more than one policy, since they are not obliged to apply Safe Harbour standards to data collected in the US. Moreover, the FTC has given assurances that companies cannot "hide behind" their published policies which do <u>not</u> relate to or reflect their adherence to the Safe Harbour. Nevertheless, the overall effect is that individuals may not know what rules apply to the processing their data, or how they can exercise their legitimate rights.

(d) Do the dispute resolution bodies named by Safe Harbour participants meet the requirements of the principles and FAQ 11?

FAQ 11 requires that participants in the Safe Harbour choose dispute resolution bodies that provide individuals with full and readily available information about how the dispute resolution procedure works when individuals file a complaint. Such information should include notice about the mechanism's privacy practices in conformity with the Safe Harbour Principles. With the exception of the Enforcement Principle, dispute resolution mechanisms are required to conform to the Safe Harbour Principles.

The Commission services have raised with the US Department of Commerce the fact that dispute resolution bodies may be operating without making any public statement as to their intention to enforce Safe Harbour rules and/or without having in place privacy practices that are in conformity with the Principles. At the time of writing of the six dispute resolution bodies presently operating in the Safe Harbour, two have self-certified to the Department of Commerce their adherence to the Principles (TRUSTe and the Entertainment Software Rating Board). Of the remaining four, two have made public statements to the effect that they act as dispute resolution bodies for organisations in the Safe Harbour (BBBOnline and the Direct Marketing Association Safe Harbour Program). The two remaining bodies, the Judicial Arbitration and Mediation Service (JAMS) and the American Arbitration Association, have done neither, but each has so far been nominated by only one organisation.

Dispute resolution bodies are also required, on the basis of FAQ 11, to ensure that the result of any remedies provided is that the effect of non-compliance with Safe Harbour rules is reversed or corrected by the organisation and that any future processing is in conformity with Safe Harbour rules. In order to be effective, such bodies need to be able to rely on a range of sanctions. It is up to the dispute resolution body to decide which sanction to use in which case, but the range of possible sanctions has to include publicity for findings of noncompliance and the requirement to delete data in certain circumstances. Other sanctions can include suspension or the removal of a seal, compensation for individuals for losses incurred and injunctive orders. Private sector dispute resolution mechanism must notify failures of Safe Harbour organisations to comply with their rulings to the government body with applicable jurisdiction, or to the courts as appropriate, and to the Department of Commerce.

The capacity to apply sanctions rigorous enough to ensure compliance with the Principles is an important aspect of the contribution dispute resolution bodies make to the soundness of the Safe Harbour. The Commission's services have reviewed the existing array of sanctions presently available to the four dispute resolution bodies that have publicly undertaken to operate as dispute resolution bodies for the Safe Harbour and concluded that all have in place means to ensure that non-compliance is corrected or reversed. This said., not all such bodies undertake to publicise their findings (only DMA and BBBOnline undertake to do so).

Conclusions

The information provided above shows that:

- All the elements of the Safe Harbour arrangement are in place.

- Compared with the situation before it was available, the framework is providing a simplifying effect for those exporting personal data to organisations in the Safe Harbour and reduces uncertainty for US organisations interested in importing

data from the EU by identifying a standard that corresponds to the adequate protection required by the Directive.

- Individuals are able to lodge complaints if they believe their rights are been denied, but few have done so and to the Commission's knowledge, no complaint so far remains unresolved.

- A substantial number of organisations that have adhered to the Safe Harbour are not observing the expected degree of transparency as regards their overall commitment or the contents of their privacy policies. Transparency is a vital feature in self-regulatory systems and it is necessary that organisations improve their practices in this regard, failing which the credibility of the arrangement as a whole risks being weakened.

- Dispute resolution mechanisms have in place an array of sanctions to enforce Safe Harbour rules. These mechanisms have not yet been tested in the Safe Harbour context. Not all of them have indicated publicly their intention to enforce Safe Harbour rules and not all have put in place privacy practices applicable to themselves that are in conformity with the Principles, as required by Safe Harbour rules. Given the importance of enforcement and the role of these bodies in it, it is necessary that Safe Harbour organisations use only dispute resolution mechanisms that fully conform to Safe Harbour requirements.

The Commission's recent Decisions approving standard contractual clauses for the transfer of data to third countries in no way affect the validity of the Safe Harbour arrangement, which should remain an attractive option for eligible organisations regularly involved in data transfers. In contacts with their US counterparts the Commission's services have underlined the need for a rigorous respect of the transparency requirements of the Safe Harbour. The Commission's services and the US Department of Commerce have agreed that transparency is a vital feature in self-regulatory systems and they look to the organisations concerned to improve their practices in this regard. They consider that some at least of the shortcomings identified can be put down to "teething problems". The Commission's services welcome the readiness of the US Department of Commerce to address some of them through improvements in the self-certification process to ensure transparency, and to provide clarification on some compliance problems. Further contacts with the DoC will be used to continue efforts to ensure that businesses are aware of the rules and that they understand that they should comply with them in a way that ensures in turn that individuals know what their rights are and how to exercise them.

The Safe Harbour arrangement is a voluntary one, but is not purely self-regulatory: it has the underpinning of US law and is subject to the vigilance and enforcement action of the relevant public authorities in the US. Such action, particularly with regard to any persistent shortcomings as identified in this report, will ensure that the arrangement will remain credible and serve its purpose as a guarantee of adequate protection for personal data transferred from the EU to the US.

The Commission services will continue to co-operate with their US counterparts in order to encourage US organisations to join and to ensure a high level of understanding of and compliance with the Safe Harbour rules and are pleased to note that the Federal Trade Commission, in public statements and in correspondence connected with the preparation of this report, has confirmed its intention to give high priority to enforcement in the area of

privacy.

(http://europa.eu.int/comm/internal_market/en/dataprot/news/02-196_en.pdf)