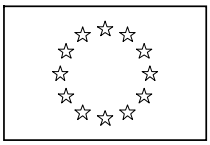

COMMISSION OF THE EUROPEAN COMMUNITIES

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 Belgium, a Royal Decree on

---

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

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 protection offices in the Member States provide information through their web sites about the Safe Harbour arrangement (UK, NL,FR, DE, IRE, IT, SW, FI and GR). None has at present a link

---

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 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-A4@cec.eu.int

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 in 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.

(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 arrangements outside the EU. The services also carried out their own information-

---

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.

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-à-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-à-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 non-compliance 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.