EU review identifies holes in US Safe Harbor scheme

THE EUROPEAN COMMISSION'S recent progress report on the US Safe Harbor scheme has expressed a mixed verdict on its implementation. Despite identifying several areas for improvement, the Commission still retains a positive attitude towards the scheme. However, a leading authority on the subject considers the Commission has minimised the scheme's weaknesses and played down the fact that the programme is seriously flawed.

On February 14th, the European Commission submitted a Staff Working Paper on the Safe Harbor scheme in working practice to the European Parliament. The paper reveals that few companies, either high profile or otherwise, have signed up to the scheme, and that the majority are failing to adhere to all of the seven principles required for providing adequate data protection.

The Safe Harbor scheme commits US organisations who sign up to adequately protect personal data – including customer and/or employee information – that is transferred from the EU to the US. Launched in November 2000, in order to achieve a safe and simplified means for transferring personal information, the scheme has attracted only around 150 companies by mid-February.

The Commission concedes that although Safe Harbor has made a fair start, it believes there is much room for improvement, stressing the need for more transparency in company privacy policies as a vital area to be addressed. However, Professor Joel Reidenberg, of Fordham University Law School, New York, considers the Commission has minimised its negative findings. Reidenberg, an expert commentator on the Safe Harbor scheme, says it is seriously flawed and that even major companies are failing to adhere to the full range of data protection principles in their self-certifying submissions to the Department of Commerce. Furthermore, he argues that the Federal Trade Commission's (FTC) claimed enforcement role is illusory because it is unlikely to be able to take action against companies under its deceptive powers law.

PL&B presents two separate views on the Safe Harbor scheme, through published extracts from the Commission's Staff Working Paper, and a response from Professor Reidenberg.

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

• All the elements of the Safe Harbor arrangement are in place. The framework is providing a simplifying effect for those exporting personal data to the 129 US organisations in the Safe Harbor 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 have 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 Harbor 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 Harbor rules exist under dispute resolution mechanisms. But not all dispute resolution mechanisms have indicated publicly their intention to enforce Safe Harbor rules and not all have in place privacy practices applicable to themselves that are in conformity with the Principles, as required by Safe Harbor rules. Enforcement is a key element in the Safe Harbor framework and it is therefore necessary that Safe Harbor organisations use only dispute resolution mechanisms that fully conform to Safe Harbor 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 Harbor 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 Harbor. 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.

Conclusions from the staff working paper

The information provided above shows that:

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

Is "visible" material provided on their web sites by organisations that have adhered to the Safe Harbor in conformity with their Safe Harbor 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 Harbor 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-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 Harbor:

Statement of adherence to Safe Harbor Principles and/or relevant privacy policy not systematically visible

To enjoy the benefits of the "Safe Harbor", companies must register with the US Department of Commerce and publicly declare their adherence to the Safe Harbor principles. Although there are in principle other ways of qualifying, at present all organisations listed qualify for Safe Harbor rights exclusively through self-regulatory efforts. To do so in compliance with Safe Harbor 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 Harbor Principles where this policy can be viewed by the public. FAQ 6 requires that "All organizations that self-certify for the Safe Harbor must… state in their relevant published privacy policy statements that they adhere to the Safe Harbor 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 Harbor 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 FTC 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 Harbor 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...

Privacy Policies do not systematically reflect Safe Harbor Principles

Less than half of organisations post privacy policies that reflect all seven Safe Harbor Principles. Some Safe Harbor 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 Harbor 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 Harbor 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 Harbor 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 Harbor obligations. The recommendation in the above-mentioned DoC Workbook is exemplary and the approach followed by the minority of Safe Harbor 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 Harbor. 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 Harbor. There is nothing in the Safe Harbor 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 Harbor standards to data collected in the US. Moreover, the FTC has given assurances that companies cannot "hide behind" their published policies which do not relate to or reflect their adherence to the Safe Harbor.

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.