Library Briefing
Library of the European Parliament 19/01/2012

The EU-US Safe Harbour Agreement

SUMMARY *The EU and the United States have very different philosophies on social regulation. One area in which this has been clearly demonstrated is e-commerce, and specifically the importance attached to data protection.*

This issue was brought to a head by the 1998 EU Data Protection Directive which required third countries, such as the US, to provide an equivalent "adequate" level of protection when dealing with data transmitted there from the EU.

Following two years of negotiations, a Safe Harbour Agreement was signed between the two parties in 2000. It required US companies who wished to transfer data from the EU, to self-certify that they complied with the agreed privacy principles and with the accompanying enforcement procedure.

The effectiveness of the Agreement was closely monitored not only from a data protection standpoint but for its wider potential as a model. Opinion, however, is divided on its success. The EU, in two early assessments, expressed concerns regarding the transparency of companies' privacy policies. Furthermore, more recent opinions also cast doubt on both actual compliance and effective enforcement.

In response, the US Department of Commerce has strongly rebutted these criticisms. It points out that self-certifying companies take compliance very seriously. In addition it argues that the Agreement has played a crucial role in fostering a greater acceptance of the importance of data protection in the US.

In this briefing:

Background

The EU and the United States represent diametrically opposed philosophies to regulating social issues such as health, safety and the environment. Whereas the EU tends to foresee a wide role for the state, the US prefers to leave more responsibility in the hands of market forces and private actors. This is particularly evident in the area of e-commerce and in the correct weighting to be given to data protection concerns.

In the late 1990s, the Clinton Administration's Framework for Global Electronic Commerce proposed industry self-regulation, along with technological solutions, as the appropriate means of ensuring data privacy. This approach, however, was at odds with EU policy and specifically the 1998 EU Data Protection Directive (DPD).

The DPD, which harmonised personal data protection across EU Member States (MS), also held non-EU countries to the same "adequate" level of protection (Article 25) when dealing with EU data transmitted and used there. US legislation was significantly inferior in comparison, and was deemed not to provide adequate protection by the independent working party set up by the European Commission. US firms that wished to trade with the EU were thus placed in a difficult situation: either they must take on the costs of meeting EU standards or risk the blockage of information regarding EU citizens. [1]

Author: Nicholas Copeland
E-mail: nicholas.copeland@europarl.europa.eu **Tel:** 32695

Towards Safe Harbour

Initial negotiations at official level were difficult. The EU, which had suspended its right to interrupt data flow to the US, was unsatisfied with the US's self-regulatory model. It wanted the US to introduce legislative changes, in line with the non-binding OECD guidelines (from 1980) that the US had previously agreed, and to accept EU-style enforcement.

Despite the support of US privacy and consumer associations, the US was unwilling to consider such action. Instead it attempted to argue the reasonableness and "adequacy" of its general sectoral approach to data protection whilst concurrently encouraging interested companies to create a functional equivalent to the EU directive.

Article 25(1) Data Protection Directive

The Member States shall provide that the transfer to a third country of personal data which are undergoing processing or are intended for processing after transfer may take place only if, without prejudice to compliance with the national provisions adopted pursuant to the other provisions of this Directive, the third country in question ensures ***an adequate level of protection***.

To break the impasse, the US Department of Commerce proposed a voluntary self-regulatory programme which would give US companies which agreed to certain rules, procedures and enforcement procedures, "safe harbour" from the EU Directive.

In order to address continuing EU concerns over self-regulation, US government and corporate officials also began to participate in business backed "web-seal programmes" such as TrustE which provide third-party seals of approval to web sites complying with certain standards. In addition, the Federal Trade Commission (FTC) increased its enforcement of unfair or deceptive company privacy policies. [2]

Although some EU MS continued to press for definitive US legislative action, even at the price of no deal, an agreement was finally reached in 2000. The decision to allow enforcement to take place in the US had the effect of upgrading the safe harbour from a presumption to a finding of adequacy under Article 25 DPD.

There nevertheless remained uncertainty as to how effective the agreement would be in practice in achieving that "adequacy", and how workable the rules and requirements would be from the perspective of private companies.

How does it work?

The Safe Harbour Agreement (SHA) is a collection of documents: seven privacy principles (see box below), 15 frequently asked questions and answers, the European Commission's adequacy decision, an exchange of letters between the US Department of Commerce and the European Commission, and letters from the US Department of Transportation and the FTC concerning their enforcement powers.

Firms signing up to the agreement are considered to be providing "adequate protection" for the data they import. This means that they agree to abide by both the principles and the accompanying enforcement procedures.

Enforcement

There is a three-pronged approach to enforcement in which self regulation is enhanced, at the insistence of the EU, by formal state mechanisms:

- Organisations may choose to resolve complaints through an alternative dispute resolution (ADR) mechanism or to cooperate directly with EU data protection authorities.
- The FTC can take action, including issuing large fines for firms acting in breach of stated privacy policies. At the time of the agreement, the FTC pledged to prioritise non-compliance with the SHA as well as referrals from certain ADR bodies.
- European data protection authorities may also act to block a data flow if the FTC or

Author: Nicholas Copeland
E-mail: nicholas.copeland@europarl.europa.eu **Tel:** 32695

an ADR reports a violation of the SHA. More generally, the EU retains the right to revoke the entire Agreement if it deems the protection offered is no longer "adequate".

The Agreement in action

In 2000, EP President Pat Cox remarked that, if the Safe Harbour Agreement proved successful it could serve as "a template for the future" with application outside the narrow area of privacy and data protection. [3]

The initial response from US companies to the SHA was however muted. In the first month only three companies signed up, and after 18 months only a small number had joined, although these did include some major international firms such as Microsoft and Hewlett Packard. From the US side, one suggestion is that this low participation was due to the unpredictability in MS enforcement of national data protection laws or even lack of knowledge of the data protection framework in the EU.

Since then the number of companies self-certifying has risen steadily with over 2 500 currently included.

The seven Privacy Principles

1. **Notice** - Individuals must be informed that their data is being collected and how it will be used.

2. **Choice** – Individuals must have the option to choose whether their information is disclosed to a third party or whether it is used for a purpose other than that for which it was collected or subsequently authorised.

3. **Onward transfer** – organisations transferring data to a third party must ensure that they also offer an equivalent level of privacy protection.

4. **Security** – Organisations must take reasonable precautions to ensure personal data is not lost, misused, disclosed, altered or destroyed.

5. **Data integrity** – Data must be relevant and reliable for the purpose for which it is used.

6. **Access** – Individuals must have access to the information collected about it and, with exceptions, be able to correct, delete or amend it where it is inaccurate.

7. **Enforcement** – Mechanisms must be available and affordable, have follow-up procedures and create obligations to remedy problems resulting from failure to comply with the Principles.

Early assessments

The Commission's first review of the implementation of the Agreement in 2002 indicated that it was simplifying and reducing uncertainty for both importers and exporters of personal data from the EU. It however expressed concern about the transparency of privacy policies and the ADR mechanisms available.

A second review in 2004 was more in-depth and focused on 41 organisations, 10% of those which had self-certified under the SHA. Although it noted a steady and encouraging increase in self-certification, it also reiterated earlier concerns relating to the content and transparency of privacy policies. In particular it noted that companies were not incorporating the seven principles. It also highlighted weaknesses in some of the ADR bodies including the failure to provide appropriate sanctions for non-compliance.

More recent criticisms

These concerns have not gone away, with one recent study finding fault both in the compliance with the EU's "adequacy" requirements and in the accuracy of the Department of Commerce's figures.

It firstly suggested that the number of member companies was severely overstated because the figure included companies which had not renewed their certification for a period of more than six months. These represented over 25% of the total stated figure.

The study also assessed compliance with the SHA's framework structure. It found that only a quarter of companies[4] met the most basic requirements and that many did not have a public privacy policy or that if they did they failed to mention Safe Harbour. It also found problems with false claims of membership and certification, as well as a widespread failure to identify an independent dispute resolution procedure for consumers. In response,

Author: Nicholas Copeland
E-mail: nicholas.copeland@europarl.europa.eu **Tel:** 32695

however, the Department of Commerce has questioned the "credible evidence" to support these conclusions and the methodology used.

The study concluded that the US's ability to protect privacy through self-regulation accompanied by regulatory oversight was questionable and that immediate improvements were required. In this light it recommended the EU take a more "hands-on" approach including re-negotiation of certain aspects of the Agreement and warning EU consumers and businesses of the need to check actual membership.

The *Düsseldorfer Kreis* decision

Similar concern and advice was expressed in April 2010 by the informal group of data protection authorities from the German *Länder*. Its decision states that companies cannot rely on self-certification as it is not effectively regulated by EU or US authorities.

It called on German data exporters to perform a due diligence check as to whether US companies, claiming to be within the Safe Harbour, are genuinely conforming or even whether their certification is valid. If such a check reveal discrepancies the decision called for exporters to use other means such as model contracts to ensure adequate protection. [5]

But a strong US rebuttal

The Department of Commerce has also mounted a strong defence of the Agreement's worth pointing out that the Safe Harbour has now grown to include over 2 500 self-certified organisations, with approximately 50 companies seeking certification each month.

It also argues that it has evolved over the past 11 years and is now considerably more sophisticated. It points out that companies spend significant amounts of money complying with the Safe Harbour indicating that it is viewed as much more than a simple "box checking" exercise.

With regard to compliance, it argues that economically it is in a company's interest to comply: a study of multinational organisations estimates that the cost of compliance generally (i.e. not just with the DPD) is more than three times less than that of non-compliance.

From a wider perspective, the Department of Commerce also claims that the SHA has played a crucial role in fostering greater acceptance of the importance of data protection in the US. As evidence, it cites both anecdotal evidence and discussions with "privacy officers" at several international firms.

Main references

H Farrell, Constructing the International Foundations of E-Commerce – The EU-US Safe Harbor Arrangement, *International Organization*, 57, Spring 2003, pp. 277–306.

M Long & M Quek, Personal data privacy protection in an age of globalisation: the US-EU safe harbor compromise, *Journal of Public Policy*, 2002, 9, 3, 325.

Disclaimer and Copyright

Endnotes

[1] Although Article 26 DPD provides derogations from the "adequacy" requirement, it was not considered to be provide sufficient protection for US companies from EU enforcement action.

[2] Section 5(a) of the Federal Trade Commission Act.

[3] Speech by Pat Cox, 8 September 2000.

[4] The study found that only 348 out 1,597 companies met the basic compliance standards.

Author: Nicholas Copeland
E-mail: nicholas.copeland@europarl.europa.eu **Tel:** 32695