TACD

TRANS ATLANTIC CONSUMER DIALOGUE
DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. ECOM-20-00 DATE ISSUED: 30 MARCH 2000

SUBMISSION OF THE TRANS ATLANTIC CONSUMER DIALOGUE (TACD) CONCERNING THE U.S. DEPARTMENT OF COMMERCE DRAFT INTERNATIONAL SAFE HARBOR PRIVACY PRINCIPLES AND FAQS, PUBLISHED ON MARCH 15, 2000.
(See paper Ecom-11-99)

BACKGROUND

On December 3, 1999, the TACD submitted comments on the U.S. Department of Commerce "Safe Harbor" Proposal of November 15, 1999. At that time, the TACD opposed the proposal since it would have failed to protect the privacy interests of consumers. The most recent draft of the Safe Harbor Proposal represents some movement forward. Consistent with our earlier recommendations, the current principles are modeled more closely on the EU Data Protection Directive and the 1980 Organization for Economic Co-operation and Development (OECD) Privacy Guidelines.

However, the current Safe Harbor proposal would still provide European citizens with inadequate protection with respect to the processing of their personal data than they are guaranteed under the EU Data Protection Directive. It is our continued view that a stronger framework with a clear enforcement mechanism must be established to protect the privacy interests of all consumers.

The EU and US at this point in time have different approaches to privacy and data protection. Under the EU Directive, privacy is a matter of legal right; there are legal limits as to the extent to which personal data can be collected and used, and there is a system of enforcement by public authorities, over and above any redress consumers might be able to pursue under their own initiative. In the US, privacy and data protection are too frequently seen as matters of industry self-regulation. Ultimately, companies can do what they like with personal data provided they can be said to have the consumers' consent. The real danger here is that consent clauses can be cleverly drafted to give companies almost a free hand to process data as they wish. In practice, consumers are forced to accept the companies' terms or otherwise lose the opportunity to do business with the company (or any other company) at all. We are therefore faced with a situation in which the US regime is currently based on a different philosophy and on a different form of

enforcement. There is no way in which the US Safe Harbor system can at present give the same level of privacy protection as in the EU. The self-regulatory system has so far proved unsuccessful in the US and we have little confidence in its effectiveness for protecting the personal information of EU citizens.

Against this background and subject to these broad reservations, TACD hereby comments on the current text of the revised Safe Harbor Arrangement.

COMMENTS

In our December 3 submission, we felt the need for stronger access, notice and consent principles backed by a legal enforcement procedure. The principles set out in the draft agreement represent a substantial improvement in many of these areas. However, many of our earlier criticisms still apply and we continue to believe that the principles outlined in the revised Safe Harbor Arrangement do not adequately establish fair information practices. The particular shortcomings of the current text are outlined below and recommendations for change suggested.

1. Enforcement

Without systematic enforcement and clear disincentives, there are no satisfactory guarantees that American companies may not violate their declared privacy practices.

<u>Self-certification and Verification.</u>

Under the current proposal, the benefits of joining Safe Harbor are granted at the time of self-certification. There is no review or independent requirement of compliance before the Safe Harbor status is granted. In addition, verification of compliance with Safe Harbor principles can be done either through self-assessment or through outside reviews. The former does not provide any substantial reassurance that compliance is taking place and the latter does not make the review or the identity of the agency conducting the review easily available.

<u>Individual complaints.</u>

The Safe Harbor enforcement principles do not provide satisfactory procedures for consumers when they have a grievance. If a company self-certifies with the Department of Commerce, it is obliged to inform the consumer of the alternative dispute resolution (ADR) body or other independent recourse mechanism to which consumers can address complaints. However, it is not clear what consumers can do if they are not satisfied with the outcome.

Also, in stark contrast to the current protections offered by the EU Data Protection Directive where individuals are granted a specific right to judicial remedy and data protection authorities are obligated to follow up on those complaints, the FTC is not required to pursue the claims of any individual consumers.

Remedies and Sanctions.

Civil penalties or sanctions for one-time or persistent violations of Safe Harbor principles may only be assessed by the Federal Trade Commission (FTC) after being referred via industry-funded self-regulatory groups such as TRUSTe or BBBOnline, ADR bodies, or data protection authorities in EU member countries. Despite past cases where individual privacy has been compromised, no self-regulatory group has ever referred a member company for investigation and the FTC has never provided remedies for any of the companies with which they have reached settlements.

Serious remedies for individuals and sanctions for companies are necessary to ensure compliance. It is hard to envisage the circumstances under which an individual would be willing to pursue a privacy complaint under the Safe Harbor Arrangement if there is no assurance of remedy or compensation.

Recommendations:

… Individual Complaints: The FTC should be obligated to follow up on consumer complaints and secure compensation for violations of the Safe Harbor principles. In addition, individuals should be specifically granted a right of remedy which could be invoked where the self-regulatory or administrative bodies fail to act or secure compensation.

Mandatory registration.

The current version of the Safe Harbor Proposal does not clearly and unambiguously state that all companies self-certifying with the arrangement must provide a letter to the Department of Commerce. All companies seeking to benefit from Safe Harbor must make their membership in the arrangement widely and publicly known.

Prior and Periodic Review of Compliance

The self-certification process does not ensure a prior acceptance of standards. There should be an independent review process to assess compliance with the principles before registration is allowed and the Safe Harbor seal granted. In addition, there should be systematic auditing of companies to determine whether companies are adhering to the principles in practice. This process should include publicly posted results of the investigations, in order to inform consumers of the disposition of their personal information.

2. Notice

Notice of privacy practices should always take place before the collection of personal information. The concession of notice until a time "as soon thereafter as is practicable" allows for the collection of information to occur without notice of the individual, and is inconsistent with the EU Directive and OECD Guidelines. While notice is now a more stringent requirement if information is to be used for different reasons or transferred to a third party, the current principle still allows collection of data before notice has been given. Also, there is no specific requirement that consumers must be informed explicitly of their right of access to their personal data.

Recommendation:
Notice of privacy practices and the rights afforded of consumers should always be provided before data collection.

3. Choice

Under the current proposal, opt-out choice is currently provided to a data subject where their personal information is used for a purpose that is incompatible with the purpose for which it was originally collected. This contrasts with the EU Directive which grants the right to object to 'before personal data are disclosed for the first time to third parties' regardless of the use to which it will be put. In addition, the Safe Harbor principles even allow for opt-out to not immediately go into effect when information is collected.

The current standard of opt-in for "sensitive information" is in accordance with Article 8 of the Directive. However, the specific wording of the principle again gives undue deference to commercial interests as it applies only to information "specifying" rather than "revealing" subjects such as medical conditions, race, or political beliefs. Clearly, no sensitive information about individuals should be collected or used and allowing a more narrow definition such as "specifying" would likely allow such practices to take place.

Recommendations:

Data subjects should have the right to object before the disclosure of their data to third parties. In addition, as the collection and use of sensitive data can result in the greatest harm to consumers, the category of data that qualifies as sensitive should be construed as broadly as possible.

4. Access

The exceptions for providing access are too broad and unfairly limit individual access in favor of business interests. While rights to access should be weighed in balance with other considerations, the current access principles allow the entities least likely to consider the rights of the data subject - the data collector - to make that determination. The current access principle allows for numerous situations for refusal to access on the basis of expense or burden , due to protection of "confidential commercial information", or for research or statistical purposes . The access principle provides for the right to have data deleted only in the case of inaccurate data and not where data is collected or processed without the subject's consent or in a way that is incompatible with that consent or with the original purpose for which the data was collected.

Recommendations:
Exceptions to the right of access should be more narrowly drawn and data subjects should be granted the right to have data deleted in all the circumstances outlined above.

5. Onward Transfer

Provisions on transfer to third parties outside the Safe Harbor system are unacceptably weak in that they allow the transfer of personal data to third parties, which do not subscribe to Safe Harbor as long as that third party signs an agreement to protect the data. Such a situation is plainly untenable and gives rise to questions concerning enforcement and liability for the wrongful use of data by that third party.

Recommendations:
The Principles should prohibit disclosure of data to third parties which do not subscribe to the principles, except where the data subject has given his or her consent.

6. Data Integrity

The purposes for which personal information is collected should be revealed before data collection and limited to such use. The Principles fail to provide adequate assurance that the information collected is not excessive, and stored only as long as necessary for the purposes for which it is collected, and kept in an anonymous form. In addition, while the Data Integrity principle now recognizes that "personal information must be relevant for the purposes for which it is to be used", the principles still allow for the transfer of information to third parties even if this does not relate to the original reasons for which it was collected. The concept of

finality -- that information provided for a specific purpose will only be used for that purpose -- is therefore not adequately provided.

Recommendation:
The text should include stronger Purpose Specification and Use Limitation principles, especially with regard to how those may include data transfer to third parties.

7. Right to Conduct Business

There is currently no prohibition on refusal of service if an individual does not provide information that he or she finds unnecessary to reveal.

Recommendation:
The Safe Harbor principles should provide the individual with protection from companies who choose to discriminate against data subjects who refuse to comply with unnecessary disclosure of their data.

CONCLUSIONS AND FURTHER RECOMMENDATIONS

1. Incorporation of the above recommendations is necessary to qualify the Safe Harbor arrangement as adequate under article 25.6 of the EU Data Protection Directive. The current proposal would undermine the purpose of the EU Data Directive and compromise the privacy interests of European citizens.

2. Of these recommendations, the Safe Harbor negotiators should consider the provision of an individual right of remedy a priority. The Directive recognizes data protection as a fundamental right that does that can be exercised by the data subject as well as by regulatory agencies.

3. The TACD should be given an opportunity to comment on the next draft of the Safe Harbor Proposal before any final decision is made. As an international coalition of over sixty American and European consumer protection groups, our expertise and interests should be brought into future steps of the negotiations.

4. In light of the considerable reservations on the effectiveness of the Safe Harbor system for protecting the personal information of EU citizens, any agreement reached between the EU and the US should be time limited. There should be provision for a full independent audit of the system, including a new determination of the adequacy, or otherwise, of the US regime, prior to the end of that period. For reasons to do with the EU system of qualified majority, it is important that the agreement is subject to this fixed time limit and not merely subject to periodic review. This will ensure that a qualified majority is required to continue the agreement after the time limit.