TACD

TRANS ATLANTIC CONSUMER DIALOGUE

DIALOGUE TRANSATLANTIQUE DES CONSOMMATEURS

DOC NO. ECOM-11-99

DATE ISSUED: DECEMBER, 1999

COMMENTS ON THE US DEPARTMENT OF COMMERCE "SAFE HARBOR" PROPOSAL OF NOVEMBER 15 1999

1. **Privacy is a human right not subject to commercial concern.** While the Safe Harbor principles were drafted with the sole purpose 'to foster, promote, and develop international commerce"[1], the European Union Data Protection Directive ("the Directive") also takes into account the human right dimension of privacy protection. Chapter 1, Article 1 of the Directive ("Object of the Directive") notes that "Member States shall protect the fundamental rights and freedoms of natural persons, and in particular their right to privacy, with respect to the processing of personal data." The drafting of Safe Harbor principles by a US agency solely concerned with the international trade implications of privacy protections will not give due weight to the importance of such protections for individuals as right-bearing citizens. Documents produced by agencies with broader social considerations have given privacy its due as a fundamental human right. Both Article 12 of the United Nations Universal Declaration of Human Rights[2] and Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms[3] directly address the need for privacy protection.

2. **Rather than eroding the principles of the Directive, Safe Harbor should seek to reinforce data protection for all individuals.** While Chapter IV of the Directive ("Transfer of Personal Data to Third Countries") merely requires an "adequate" rather than equivalent level of protections in non EU-member countries, the Directive should not be construed as an upper limit for privacy protections but as a baseline standard. The Directive states that national laws which will approximate the principles in the Directive " must not result in any lessening of the protection they afford, but must, on the contrary, seek to ensure a high level of protection"[4] Globalization of the economy necessarily exposes individuals to the laws of foreign countries and the values and principles embodied in those laws. In contrast to the fundamental right of privacy the Directive respects, the Safe Harbor principles undercut data protection (see 4) for European citizens in order to make the entry of US companies into foreign markets as painless as possible.

[1] http://www.ita.doc.gov/ecom/Principles1199.htm, Draft, International Safe Harbor Privacy Principles issued by the US Department of Commerce ("Principles"), paragraph 2, 15 November 1999.
[2] http://www.hrweb.org/legal/udhr.html.
[3] http://www.coe.fr/eng/legaltxt/5e.htm.
[4] Preamble, European Union Data Protection Directive.

3. **The Safe Harbor Agreement will provide limited data protection only for individuals residing in EU member countries.** Under the Safe Harbor principles, European citizens will enjoy greater privacy protections from US companies than any US citizen. While US companies may view the acceptance of Safe Harbor principles as an obstacle to developing European markets, US citizens should be alarmed that principles drafted by a US agency for US companies would give greater protections to citizens of another country.

4. The Principles outlined in the Safe Harbor Proposal do not adequately establish fair information practices.

5. **Notice.** Notice of privacy practices should always take place before the collection of personal information without exception. The concession of notice until a time "as soon as is practicable"[5] allows for the collection of information to occur without notice of the individual.

6. **Consent not choice.** The collection of personal information requires opt-in consent from the individual not opt-out choice. Opt-out choice unfairly places the burden of preventing the collection of personal information on the individual. Given the invisibility of new technology in the collection of personal information, consent is necessary to adequately establish control over personal information. Furthermore, the current standard of opt-in for "sensitive information" gives undue deference to commercial interests since it applies only to information "specifying" rather than "revealing" subjects such as medical conditions, race, or political beliefs.[6] Even considering the weak protection of opt-out choice, the Safe Harbor principles even allow for opt-out to not immediately go into effect when information is collected.[7]

7. **Purpose specification and use limitation.** The purposes for which personal information is collected should be revealed before data collection and limited to such use. The requirements of notice and consent should apply to information which will be passed onto third parties not subscribing to Safe Harbor principles[8] or those third parties whose use of such information is "compatible"[9] with the purpose for which it was originally collected and authorized to be used. This is particularly important given the lack of responsibility that the original data collector will bear for any transgressions of the third party in processing personal information.[10] To maintain control over personal information, the individual must be aware of all purposes and use of that information. The Principles also fail to provide adequate assurance that the information collected is relevant, not excessive, and stored only as long as necessary for the purposes for which it is collected.

8. **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

---

[5] Principles, "Notice".
[6] In addition, the US Tenth Circuit Court of Appeals is currently considering a petition for rehearing in the case mentioned in the draft principles. For more information, see http://www.epic.org/privacy/litigation/uswest/.
[7] http://www.ita.doc.gov/ecom/FAQ12Opt-Out1199.htm, FAQ 12, "Choice – Timing of Opt Out".
[8] Principles, "Choice", text struck out.
[9] Principles, "Onward transfer".
[10] Principles, "Onward transfer".

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[11], due to protection of "confidential commercial information"[12], or for research or statistical purposes[13]. The access principle provides for the right to have data deleted only in case the date is inaccurate. Instead, the data subject should have the right to have data deleted whenever there has been an infringement of the Safe Harbor Principles.

9. **Oversight and enforcement.** Oversight and enforcement of these principles rely on industry self-policing which has shown itself ineffective against companies that have violated consumer privacy. Verification of compliance with Safe Harbor principles can be done either through self-assessment or through outside reviews.[14] 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 publicly available. The dispute resolution and enforcement component of the Safe Harbor principles does not provide for any civil penalties or tangible punishments as sanctions for one-time or persistent violations of Safe Harbor principles.[15] Such penalties may only be assessed by the Federal Trade Commission only after being referred via industry-funded groups such as TRUSTe or BBBOnline, neither of which have ever taken any action against a licensee deserving of a full investigation. The enforcement principle should include compensation for any damage suffered by individuals.

10. **Right of individual to conduct business.** The Safe Harbor principles do nothing to protect the individual from refusal of service if a customer does not provide information that he or she finds is unnecessary for transactions.

[11] http://www.ita.doc.gov/ecom/FAQ8access1199.htm, FAQ 8, "Access", question 1.
[12] FAQ 8, "Access", question 2.
[13] FAQ 8, "Access", question 5.
[14] http://www.ita.doc.gov/ecom/FAQ7Verif1199.htm, FAQ 7, "Verification".
[15] http://www.ita.doc.gov/ecom/FAQ11DisputeRes1199.htm, FAQ 11, "Dispute Resolution and Enforcement".