

November 1, 2004

EU Commission Safe Harbour Report

On 25 October 2004, the European Commission published its long-awaited, second report, or "Staff Working Document," on the effectiveness of the EU-U.S. Safe Harbour mechanism for transferring personal data from the EU to the U.S. In this report, the Commission assesses the performance of each of four of the key Safe Harbour participants -- U.S. companies enrolled in the Safe Harbour ("Safe Harbourites"); the U.S. Department of Commerce ("DoC"); the U.S. Federal Trade Commission ("FTC"); and U.S. private sector dispute resolution bodies ("DRBs"), and offers recommendations for improving the Safe Harbour scheme.

Overall, the Commission finds the recent increased participation in the Safe Harbour by U.S. companies (now numbering more than 590) "encouraging," but questions whether the arrangement offers adequate protection to transferred personal data. The Commission's concerns arise out of a 2003-04 "visible compliance" study, which reviewed the privacy policies of randomly selected U.S. companies enrolled in the Safe Harbour and the current practices of the DoC, FTC, and DRBs involved in resolving Safe Harbour disputes.

It remains far too early to predict whether, and if so how, U.S. authorities will respond to the criticisms contained in the Commission report, although some reaction is probable. Nor is it clear whether the report portends greater Commission scrutiny of Safe Harbour transfers in future. For Safe Harbourites, now is plainly a good time to ensure that they abide by their Safe Harbour commitments, particularly since the Commission encourages EU privacy regulators to suspend data flows where they conclude there is "substantial likelihood" that a U.S. company may be breaking the rules.

Principal Conclusions and Recommendations

The Commission's report focuses primarily on three aspects of the Safe Harbour scheme -- (i) visible compliance by Safe Harbourites with the Safe Harbour Principles; (ii) the success of the U.S. DoC in administering the Safe Harbour; and (iii) the success of the U.S. FTC, DRBs, and the specially-created EU panel in enforcing the Safe Harbour.

- Compliance by U.S. Organizations. The Commission articulates two chief concerns regarding compliance by U.S. companies with the Safe Harbour scheme. First, the Commission finds that a "substantial minority" fail to have a publicly-accessible privacy policy, a basic Safe Harbour requirement. The Commission calls upon the DoC to provide Safe Harbour participants with guidelines or best practice advice on privacy policies, and to perform periodic checks to ensure that companies make them publicly available. Second, the Commission observes that many of the privacy policies that are publicly available breach the Safe Harbour's rules relating to notice, choice, access, and enforcement. Again, the Commission requests that the DoC (and the FTC) become more active in ensuring compliance and issue guidelines or best practice advice.

More troublingly, the Commission encourages European privacy regulators to suspend data flows if they conclude that there is "a substantial likelihood" that a U.S. company is failing to abide by its Safe Harbour commitments. However, this will only be the case where the regulator reasonably believes that the company's Safe Harbour enforcement mechanism is inadequate and the continuing transfer of data would create an "imminent risk of grave harm" to data subjects, and first provides the U.S. company with an opportunity to respond to any concerns.

- Administration of Safe Harbour. The Commission appears generally satisfied with the U.S. DoC's manner of operating the Safe Harbour in the U.S., although it does find room for improvement. In particular, the Commission offers some technical suggestions for making the DoC's Safe Harbour website more user-friendly and effective, including the introduction of a new "box" where Safe Harbourites can reflect their commitment to comply with the advice of the EU enforcement panel in appropriate cases.
- Enforcement of Safe Harbour. The Commission notes some problems with the way the U.S. FTC and DRBs, in particular, enforce the Safe Harbour, while accepting that there have been extremely few Safe Harbour disputes to date. On the one hand, the Commission recommends that the FTC be more proactive in enforcement and undertake investigations of alleged Safe Harbour violations *sua sponte*, as well as clarify its authority to regulate companies using the Safe Harbour to transfer only human resources data. On the other hand, the Commission complains that certain DRBs lack transparency and may fail to remedy Safe Harbour breaches adequately. The Commission is unable to judge the performance of the EU panel, since it has not had been called upon to decide a single dispute to date.

Finally, the Commission concludes its report by finding that the Safe Harbour has not been implemented in a discriminatory manner, either with respect to industry sectors or countries. In particular, the Commission rejects claims that the Safe Harbour imposes a higher standard of privacy on U.S. Safe Harbour participants than is found in those countries that the Commission formally has deemed to provide "adequate" protection.

* * *

This information is not intended as legal advice, which may often turn on specific facts. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

If you have any questions concerning the material discussed in this client alert, please call the following co-chairs of our privacy and security practice group:

Henriette Tielemans	+32.2.549.5252	htielemans@cov.com
Erin Egan	202.662.5145	eeegan@cov.com

Covington & Burling is one of the world's preeminent law firms known for handling sensitive and important client matters. This alert is intended to bring breaking developments to our clients and other interested colleagues in areas of interest to them. If you do not want to receive alerts like this in the future, please contact us by sending an e-mail to unsubscribe@cov.com.