Privacy Regulation

Spring 2003

US/EU Safe Harbor Agreement: What It Is and What It Says About the Future of Cross Border Data Protection

The Honorable Mozelle W. Thompson[1]
Commissioner
Federal Trade Commission
Washington, DC

Peder van Wagonen Magee[1]
Federal Trade Commission
Washington, DC
pmagee@ftc.gov

In February 1999, the staffs of the United States Department of Commerce ("Commerce") and the Federal Trade Commission ("FTC" or "Commission") huddled together in an FTC conference room to discuss the European Union's ("EU") soon-to-be-implemented directive governing the collection and dissemination of personal data gathered from the citizens of its 15 member states.[2] At the time, America was in the middle of the "dot-com bubble" as consumers began to engage in e-commerce and companies found newer and more sophisticated ways to collect information about their cyber visitors. Both agencies were heavily involved with issues raised by the newly emerging global electronic marketplace: Commerce, with such issues as encryption, digital signatures and domain name registration; and the FTC with online marketing and consumer protection. It took little more than a cursory glance at the EU's new "Privacy Directive" to recognize that it could potentially block trans-Atlantic data flows. This bottleneck threatened not only to seriously hamper traditional international trade, but also to cause e-commerce to wither on the vine.

The Privacy Directive was one by-product of the European Commission's attempt at harmonizing the maze of 15 countries' laws and regulations governing a wide range of subjects - - including the gathering and dissemination of citizens' personal information. The Privacy Directive required member states to pass laws and take steps to protect the privacy of their citizens' personal data. Even more importantly, from a global perspective, the Privacy Directive also directed EU member States to prohibit transmissions of personal data to any entity that did not agree to provide similar protections.[3] This requirement created the potential for serious conflict with the United States ("US"), a country with no generally applicable law governing data protection.[4] Absent some agreement between

the US and the EU, the Privacy Directive threatened to disrupt trans-Atlantic commerce by blocking the ability of European organizations to transfer employee records, customer records and other types of personal data to companies in the United States. Neither the EU nor the US thought this was a desirable result.

The Privacy Directive's extraterritorial effect became a focus of Commerce and the FTC's attention. After several months of complex negotiations the US and the EU agreed upon an innovative framework that would act as a bridge for sharing data between the two continents, while preserving the basic policy principles of both. By establishing a self-certification

Accordingly, Commerce and the FTC sought to negotiate a safe harbor based on the following goals:

- Voluntary participation of American companies that received European data.
- Compliance standards that the US through the Department of Commerce (and not the EU) certified.
- Existing US law enforced by the FTC.

After some 17 months of discussions, in July 2000, the US and the European Union agreed upon a framework with a set of Safe Harbor Principles that satisfied each of these goals.[5]

Safe Harbor Requirements for US Companies

The safe harbor framework, including how companies can participate and certify their compliance, is set forth in detail on the Commerce and the FTC websites.[6] To summarize, the agreement allows most US corporations to certify to Commerce that the company has joined a self-regulatory organization that adheres to the following seven Safe Harbor Principles or has implemented its own privacy policies that conform with these principles. A self-certifying organization must do the following:

- Notify individuals about the purposes for which information is collected and used;
- Give individuals the choice of whether their information can be disclosed to a third party;
- Ensure that if it transfers personal information to a third party, that the third party also provides the same level of privacy protection;
- Allow individuals access to their personal information;
- Take reasonable security precautions to protect collected data from loss, misuse or disclosure;
- Take reasonable steps to ensure the integrity of the data collected; and
- Have in place an adequate enforcement mechanism.

Since the creation of the Safe Harbor Principles, Commerce has certified over 300 companies as qualifying for the safe harbor. That figure includes over 6% of the Fortune 500 companies. Jay Cline, Safe Harbor: A Success, Computerworld (Feb. 19, 2003).

The Safe Harbor and FTC Enforcement Actions

It is well-settled that the FTC has authority to sue a company that makes

Lessons Learned from Microsoft Passport and Eli Lilly

Microsoft and Eli Lilly are both American companies that market to consumers worldwide. Both companies made public representations about the use and security of the personal information they collected and both were alleged to have violated their own public representations. Although neither action was specifically characterized as a safe harbor case,[9] they both provide insight into how the Commission might approach enforcement of the Safe Harbor Principles.

It is evident through these cases that the FTC will evaluate whether a company has taken "reasonable precautions" to protect the security of its consumer data, based on the sensitivity of the data at issue. This "sliding scale" – as opposed to an inflexible, a one-size-fits all approach -- can apply to other Safe Harbor Principles as well. The level of choice a company must offer its customers concerning data collection (opt-out versus opt-in) depends upon the sensitivity of the data being sought. Similarly, the judgment about the sufficiency of a company's data access program requires consideration of the type of data collected weighed against the burden and the risk to the company.

Each case will obviously be driven by its specific facts; however, it is likely that judgments about reasonableness will differ where the data involved is financial, medical, or some other type of highly sensitive information. Therefore, these questions could form the basis for future actions where there is a claim of breach of the Safe Harbor Principles.

Conclusion

With this background in mind we can provide some advice for those who are counseling organizations that collect, receive, or otherwise use consumer information. First, they should advise their clients to identify whether the client collects or receives personal information from consumers and, if so, what kind of information it is.[10] Second, they should advise organizations that collect or receive data from EU citizens to strongly consider applying for safe harbor certification. While certification requires that the organization take some responsibility for how it collects and uses personal data, this exposure is likely to be far less serious than the risk of facing legal actions brought by each of the 15 EU Data Commissioners.[11] Finally, an organization should take steps to ensure that it is fulfilling its privacy policies, whether or not it is certified through the safe harbor. This last point is important not only because of the risk of FTC enforcement, but also because it makes good business sense.

(Endnotes)

1 Mozelle W. Thompson is a Commissioner at the United States Federal Trade Commission. He participated in the negotiations leading to the US/EU Safe Harbor Principles and agreement as head of the United States Delegation to the Organization for Economic Cooperation and Development Consumer Policy Committee. Commissioner Thompson now serves as Chairman of the Committee. Peder Magee is Attorney Advisor to Commissioner Thompson, working on various consumer protection and competition matters with specific emphasis on online privacy, global e-commerce, and high technology matters. The views expressed in this article are those of the authors, and do not necessarily reflect the views of the Federal Trade Commission or any other individual Commissioner or Commission employee.

2 The EU members include Austria, Belgium, Denmark, Finland, France, Germany, Greece, Italy, Ireland, Luxembourg, The Netherlands, Portugal, Sweden, Spain, and the United Kingdom.

3 "Member States shall provide that the transfer to a third country of personal data . . . may take place only if . . . the third country in question ensures an adequate level of protection." Council Directive 95/46/EC,062 Tw[(U)27.(T9s12.2ceon ensur)o0106 T19 Tc16(e)Tn3h5qua