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 process that incorporated seven required privacy policy elements, this "safe harbor" agreement allowed the data of European citizens to continue to flow to certain American companies.

This article provides a glimpse of the circumstances that surrounded the US and European safe harbor negotiations, summarizes how the safe harbor operates today, and provides guidance concerning future US action in the privacy area.

US Goals In The Safe Harbor Negotiations

In negotiating the substance of the US/EU Safe Harbor Principles, the US sought to advance certain policy goals. After examining the EU Privacy Directive and recognizing its potential impact on trans-Atlantic trade, Commerce and the FTC began to explore how to address the EU's data protection concerns while at the same time, respecting the sectoral approach of US data protection laws. Both agencies already believed that encouraging industry self-regulatory efforts in the online privacy area was good for consumers and good for e-commerce. Indeed, the US had already agreed to the 1988 Organization of Economic Cooperation and Development's ("OECD") Privacy Principles, and many US companies had already adopted some form of these nonbinding principles through participation in several self-regulatory bodies. (See e.g., The Online Privacy Alliance, Trust-E and BBB Online). Moreover, the FTC's authority under Section 5 of the Federal Trade Commission Act ("FTCA") to take action against unfair or deceptive trade practices, as well as the agency's strong enforcement background, provided a clear statutory and historical backdrop to bolster industry self regulation.

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 public representations which it fails to fulfill. See e.g., Deception Policy Statement, Cliffdale Associates, Inc., 103 F.T.C. 110, 176 (1984). The Commission has also determined that this authority extends to a company's violation of its privacy policy or other misrepresentations concerning its information practices. See Toysmart.com,, Civil Action No. 00-11341 (D.MA. July 21, 2000); GeoCities, Docket No. C-3849 (Final Order Feb 12, 1999). This same statutory jurisdiction will serve as the primary basis for government action against a US company that obtains safe harbor certification but fails to comply with the Safe Harbor Principles.[7] To date, Commerce and the FTC have not received any complaints about privacy breaches committed by any of the registered American companies. Notwithstanding this lack of complaints, however, the FTC has increased its privacy enforcement activities, and two recent actions illustrate how the Commission might pursue safe harbor enforcement.

Microsoft Passport

In August of 2002, Microsoft settled FTC allegations that the company had made deceptive claims about the security of its Passport Internet service and about the types of customer information it collected in connection with the service. Microsoft Corp., Docket No. C-4069 (Final Order Aug. 8, 2002). Microsoft's Passport system collects and maintains consumers' personal information and allows consumers to use the stored data in making online purchases through participating web sites. Following an investigation, the FTC concluded that Microsoft had falsely claimed that "it maintained a high level of online security by employing sufficient measures reasonable and appropriate under the circumstances to maintain and protect the privacy and confidentiality of personal information" of its Passport consumers. Microsoft Corp., Docket No. C-4069, Complaint at para. 6. Additionally, the FTC asserted, Microsoft had deceived consumers by failing to disclose that it collected personally-identifiable, sign-in history data from its Passport customers.

In analyzing whether the Microsoft Passport security measures were reasonable and appropriate, the Commission looked closely at the nature of the underlying data. Although Microsoft did have some security measures in place to protect its customer data, because of the sensitive nature of such data -- including consumers' credit card information -- the Commission determined that Microsoft's security was insufficient. Similarly, even though Microsoft collected and retained the customer sign-in history data for only a limited time, the sensitivity of those data made the failure to disclose its collection a deceptive omission, in violation of Section 5.

The FTC settled its allegations against Microsoft when the company agreed to an order that enjoined it from misrepresenting its information practices and required it to implement and maintain a comprehensive information security program that is subject to the review and certification of an independent third-party review organization.[8] This remedy is significant because it represents the first time that a private corporation has agreed to regular, independent third party review of its privacy and information security practices in the context of a Commission order.

Eli Lilly

A second matter involving allegations of privacy violations and inadequate data security, involved the pharmaceutical company Eli Lilly ("Lilly"). Eli Lilly and Co., Docket No. 4047, (Final Order May 8, 2002). Through its Prozac.com Web site, Lilly collected personal data and offered customers its "Medi-messenger" service which sent consumers personal e-mail reminders to take or refill their medication prescriptions. Privacy policies that Lilly posted on its website stated that the company took the necessary steps to maintain and protect the privacy and confidentiality of its customers' personal information.

The Commission challenged Lilly's privacy and security claims as deceptive under Section 5 after a Lilly employee unintentionally distributed an e-mail that disclosed the identities of some 700 of Lilly's prosac.com subscribers. Despite the unintentional nature of the disclosure, the FTC determined that Lilly's internal privacy and security measures were inadequate given the highly sensitive nature of the data at issue and the express representations the company had made regarding the security of that information. The Commission further found that Lilly had failed to provide "appropriate training for its employees regarding consumer privacy and information security" and had failed to "implement appropriate checks and controls" over the prozac e-mail program. Eli Lilly and Co., Docket No. 4047, Complaint at para. 7.

The FTC's settlement with Lilly bars the company from making misrepresentations about the privacy or security of the company's consumer information. The settlement also requires Lilly to establish a four-stage information security program that identifies "reasonably foreseeable internal and external risks to security, confidentiality, and integrity of personal information." Decision and Order at para. II.

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, 1995 O.J. (L 281) 31, Article 25.

4 Unlike Europe's "top-down" regulatory approach to privacy protection, historically the US has taken a "sectoral" approach mixing self-regulation with certain discrete legislation pertaining to specific industries. See, e.g., Fair Credit Reporting Act, Gramm-Leach-Bliley Act, Children's Online Privacy Protection Act. Some would argue that these differences create the perception that European privacy protections focus more on legal principles, while America's privacy protections are more focused on enforcement.

5 It is important to keep in mind that the US and the EU are continuing to negotiate the safe harbor with respect to certain issues such as financial institutions. The current safe harbor does not apply to financial institutions and there is a de facto moratorium by the EU on pursuing financial institutions that transfer personal information to organizations in the US. The extent to which the Gramm-Leach-Bliley Act is sufficient for purposes of the Privacy Directive is an unresolved issue to which US companies and their counsel should pay close attention.

6 See United States Department of Commerce, Export Portal, http://www.export.gov/safeharbor/sh_overview.html. Financial and insurance organizations, telecommunications companies and not-for-profits are ineligible for safe harbor certification.

7 The Department of Commerce publishes a list on its website containing the names of each organization that obtains safe harbor certification (http://web.ita.doc.gov/safeharbor/shlist.nsf/webPages/safe+harbor+list). The FTC views this publication as an affirmative representation which is actionable if violated. Letter from Robert Pitofsky, Chairman, Fed. Trade Comm'n, to John Mogg, Director, DG XV, European Comm'n (July 14, 2000), available at http://www.export.gov/safeharbor/FTCLETTERFINAL.htm.

8 It is important to note that the Passport investigation did not arise from specific consumer complaints, but was instead prompted by a request from a coalition of public interest groups. Consequently, there was no provision for consumer redress.

9 Microsoft is a certified safe harbor company and the EU has looked at its Passport system; however, the Commission's allegations did not specifically concern the safe harbor.

10 Companies that collect data online from children under 13, for example, must comply with COPPA.

11 These actions can stem from violations of each country's laws governing the collection and use of personal information.