U.S. Federal Trade Commission
Staff Comments to the European Commission
on the Review of the EU Regulatory Framework for
Electronic Communications Networks and Services

December 2006

I. Introduction

Staff of the U.S. Federal Trade Commission (FTC) appreciate the opportunity to comment on the proposed changes to the European Union regulatory framework for electronic communications networks and services.[1] By soliciting public comments on proposed changes to this regulatory framework, the European Commission demonstrates its acknowledgement of the importance of an international dialogue on these issues. The FTC staff strongly believes that in this globalized marketplace, the regulatory regime in one jurisdiction necessarily affects businesses and consumers located in other jurisdictions, and accordingly international consultation is worthwhile. Our staff comments relate to two areas: (1) security measures required of providers of publicly available electronic communications services; and (2) security breach notification requirements required of these service providers.

Legal requirements relating to security measures and data breaches are important issues that the FTC deals with regularly. Under certain circumstances, the FTC has the authority to bring actions against companies subject to FTC jurisdiction for their failure to provide reasonable protections for sensitive consumer information. This authority is based both on the Federal Trade Commission Act (which prohibits unfair or deceptive acts or practices), and on a law that covers financial institutions. Using this authority, the FTC has brought fourteen actions against companies for their failure to provide reasonable protections for sensitive consumer information.[2]

---

[1] The views expressed in this comment are those of the FTC staff and do not necessarily represent the views of the Federal Trade Commission or any individual Commissioner.

[2] In the Matter of Guidance Software, Inc., FTC Docket No. 062 3057 (proposed settlement posted for public comment on November 16, 2006); In the Matter of CardSystems Solutions, Inc., FTC Docket No. C-4168 (September 5, 2006); In the Matter of Nations Title Agency, Inc., FTC Docket No. C-4161 (June 19, 2006); In the Matter of DSW, Inc., FTC Docket No. C-4157 (Mar. 7, 2006); United States v. ChoicePoint, Inc., No. 106-CV-0198 (N.D. Ga. Feb. 15, 2006); Superior Mortgage Corp., FTC Docket No. C-4153 (Dec. 14, 2005); In the Matter of

In the United States, certain institutions are subject to federal breach notification regulations, and there are certain states that have breach notification laws.[3] The FTC has been actively involved in the dialogue on legally mandated breach notification.[4]

We understand that the European Commission regulatory review relates to the electronic communications sector. Nevertheless, we believe that our more general experience in the area of legally mandated information security requirements and data breach notification might be useful as you evaluate reforms to the electronic communications regulatory framework.

II. Comments

A. Security measures required of service providers

Under the existing EU regulatory framework, providers of electronic communications services ("service providers") must take "appropriate technical and organisational measures" to safeguard the security of their services.[5] The European Commission Staff Working Document

---

BJ's Wholesale Club, Inc., FTC Docket No. C-4148 (Sept. 20, 2005); Nationwide Mortgage Group, Inc., FTC Docket No. 9319 (April 12, 2005); In the Matter of Petco Animal Supplies, Inc., FTC Docket No. C-4133 (Mar. 4, 2005); In the Matter of Sunbelt Lending Services, FTC Docket No. C-4129 (Jan. 3, 2005); In the Matter of MTS Inc., d/b/a Tower Records/Books/Video, FTC Docket No. C-4110 (May 28, 2004); In the Matter of Guess?, Inc., FTC Docket No. C-4091 (July 30, 2003); In the Matter of Microsoft Corp., FTC Docket No. C-4069 (Dec. 20, 2002); In the Matter of Eli Lilly & Co., FTC Docket No. C-4047 (May 8, 2002). Information about these actions, as well as additional actions relating to consumer privacy issues are available at http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html

[3] Institutions subject to the regulatory authority of the U.S. Federal banking agencies are required to notify their regulators as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information. In addition, notice to consumers is required when, based on a reasonable investigation of an incident of unauthorized access to sensitive customer information, the financial institution determines that misuse of its information about a customer has occurred or is reasonably possible. See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15,736-54 (Mar. 29, 2005). Also, certain states in the U.S. have breach notification laws, including California, Florida and Maine.

[4] *Data Breaches and Identity Theft: Hearing before the Senate Comm. on Commerce, Science and Transp.* 109th Cong., 1st Sess. (2005) (Prepared Statement of the FTC, presented by Chairman Deborah Platt Majoras) *available at* *http://www.ftc.gov/os/2005/06/050616databreaches.pdf*

[5] Directive 2002/58/EC (OJ L 201, 31.7.2002, p. 43). Security requirements are of course also included in Directive 95/46/EC (OJ L 281, 23.11.95 p. 43) on the protection of individuals with regard to the processing of personal data and on the free movement of such data.

contains a number of different proposals to modify the existing regulatory framework in order to "strengthen and extend existing provisions on security and network integrity."[6] One of the options is to introduce detailed technical and organisational obligations for service providers, while another option is to introduce general security and integrity requirements.[7]

Generally, the FTC advocates a strong but flexible approach with regard to mandating specific security requirements on institutions holding sensitive personal information about consumers. A flexible approach, reflecting widely accepted principles of information security, like those contained in the Organisation for Economic Co-operation and Development's Guidelines for the Security of Information Systems and Networks, provides institutions with workable guidance to assist them in developing their security safeguards.[8]

Indeed, when the FTC drafted the Safeguards Rule that established the legally mandated standards relating to safeguards for financial institutions that fall under the jurisdiction of the FTC, the goal was to develop a standard that would provide companies with the flexibility to develop safeguards appropriate to their organization.[9] The Safeguards Rule does not mandate specific technical requirements that may not be appropriate for all entities and might quickly become obsolete. Rather, the Rule requires companies to evaluate the nature and risks of their particular information systems and the sensitivity of the information they maintain, and to take appropriate steps to counter these threats. Companies are different from one another and a

---

[6] Commission Staff Working Document on the Review of the EU Regulatory Framework for electronic communications networks and services (SEC (2006) 817) 28 June 2006, p. 26.

[7] Commission Staff Working Document on the Review of the EU Regulatory Framework for electronic communications networks and services (SEC (2006) 817) 28 June 2006, p. 26.

[8] See Organisation for Economic Co-operation and Development, *Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security* (July 25, 2002), *available at* http://www.oecd.org/document/42/0,2340,en_2649_34255_15582250_1_1_1_1,00.html.

[9] Pursuant to the Gramm-Leach-Bliley Act, the U.S. law that requires financial institutions to design, implement and maintain safeguards to protect customer information (5 U.S.C. §§ 6801-09 *available at* http://www.ftc.gov/privacy/glbact/glbsub1.htm), the FTC was required to issue the Safeguards Rule (16 C.F.R. 314 (2002) *available at* http://www.ftc.gov/os/2002/05/67fr36585.pdf).

flexible approach is necessary to accommodate these differences and to allow for advances in technology. For example, some companies store personal information electronically, while others may keep paper files. Also, companies have different management structures that might affect the way they organize data security responsibilities.

The FTC has testified that it believes the U.S. Congress should consider whether new legislation incorporating the flexible standard of the Safeguards Rule is appropriate.[10] Because the Safeguards Rule does not cover many entities that may also collect, maintain, and transfer or sell sensitive consumer information, new legislation could mandate this specific requirement on these other entities.

In contemplating changes to the current regulatory framework, the FTC staff recommends that the European Commission consider flexible safeguard requirements so as to allow organizations to tailor security safeguards to their own circumstances. It is important for businesses to have the ability to structure their security safeguards in a way that is suitable to their organization.

B. Requirements on providers of electronic communications to provide notification of security breaches and to keep users informed

Under the existing EU regulatory framework, service providers are required to notify subscribers about security risks, but there is no express requirement to notify subscribers of actual security breaches.[11] The European Commission Staff Working Document contains proposed changes to the regulatory framework that would require service providers to notify customers of any security breach leading to the loss, modification or destruction of, or unauthorised access to, personal information.[12]

---

[10] *Data Breaches and Identity Theft: Hearing before the Senate Comm. on Commerce, Science and Transp.* 109th Cong., 1st Sess. (2005) (Prepared Statement of the FTC, presented by Chairman Deborah Platt Majoras) *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

[11] Directive 2002/58/EC (OJ L 201, 31.7.2002, p. 43).

[12] Commission Staff Working Document on the Review of the EU Regulatory Framework for electronic communications networks and services (SEC (2006) 816) 28 June 2006, pp. 29-30.

A uniform standard for breach notification, like the one proposed by the European Commission, can be beneficial. A uniform standard facilitates compliance, and may reduce burdens and costs to affected companies. In contemplating a standard for breach notification, the FTC staff recommends that the European Commission carefully consider whether it should require service providers under all circumstances to notify customers of a security breach. Generally, the FTC recommends that if a security breach creates a significant risk of identity theft or other related harm, affected consumers should be notified.[13] Prompt notification to consumers in these cases can help them mitigate the damage caused by identity theft. There may be security breaches that pose little or no risk of harm, such as a lost laptop that is quickly recovered before anyone can obtain unauthorized access. Requiring a notice in this type of situation might create unnecessary consumer concern and confusion. Moreover, if notices are required in cases where there is no significant risk to consumers, notices could become quite common and consumers may become numb to them and fail to spot or act on those risks that truly are significant. In addition, notices can impose costs on consumers and on businesses, including businesses that were not responsible for the breach. For example, in response to a notice that the security of his or her information has been breached, a consumer may cancel credit cards, or obtain a new driver's license number. If these actions are not warranted by the risk involved, they would impose unnecessary burdens on consumers and affected businesses.

Accordingly, the FTC staff recommends that the European Commission consider not requiring breach notification in all cases, but rather, to focus on those where there is a significant risk of identity theft or related harms. For example, if the type of personal information compromised will allow thieves to open accounts in the consumer's name, notification to the affected consumers is warranted so that they can take some steps to prevent or limit any harm.

III. Conclusion

In addition to the specific comments above, FTC staff would like to make the European Commission aware of a current initiative in the United States. On May 10, 2006, President Bush signed an executive order creating an Identity Theft Task Force, co-chaired by the U.S. Attorney

---

[13] *Data Breaches and Identity Theft: Hearing before the Senate Comm. on Commerce, Science and Transp.* 109th Cong., 1st Sess. (2005) (Prepared Statement of the FTC, presented by Chairman Deborah Platt Majoras) *available at* http://www.ftc.gov/os/2005/06/050616databreaches.pdf.

General and the Chairman of the FTC.[14] The Task Force will develop a strategic plan to enhance the effectiveness and efficiency of government efforts to deter, prevent, detect, investigate, and prosecute identity theft. This Task Force issued interim recommendations in September 2006 on measures that can be implemented immediately to help address the problem of identity theft. These interim recommendations included a recommendation that a memorandum be issued to all U.S. Federal agencies advising them on the steps to take in the event of a compromise of data. The Task Force developed and formally approved a set of guidelines that provides the factors that should be considered in deciding whether, how, and when to inform affected individuals of the loss of personal data that can contribute to identity theft, and whether to offer services such as free credit monitoring to the persons affected.[15]

These recommendations and accompanying guidelines may be generally useful to the European Commission as it conducts its review, specifically with regard to in determining under what conditions it will require data breach notification.

In closing, the FTC staff appreciates the opportunity to submit comments to the European Commission in connection with its Review of the EU Regulatory Framework for electronic communications networks and services. Please feel free to contact Hugh G. Stevenson, Associate Director for International Consumer Protection at the Federal Trade Commission, at hstevenson@ftc.gov or 202-326-3511, or Yael Weinman, Legal Advisor for International Consumer Protection at the Federal Trade Commission at yweinman@ftc.gov or 202-326-3748, if you have any questions or would like any additional information about the issues raised in this Staff Comment.

---

[14] See *http://www.whitehouse.gov/news/releases/2006/05/20060510-6.html*

[15] See FTC press release announcing these interim recommendations, and the recommendations *available at* http://www.ftc.gov/opa/2006/09/idtheft.htm.