U.S. Federal Trade Commission Staff comments on the European Commission's November 2010 Communication on Personal Data Protection in the European Union[1]

January 13, 2011

I. Introduction

United States Federal Trade Commission (FTC) staff submits the following comments to the European Commission (EC) on the November 2010 *Communication from the Commission to the European Parliament, the Council, the Economic And Social Committee and the Committee of the Regions - A Comprehensive Approach On Personal Data Protection In The European Union* (EC Communication) on modernizing the European Union's (EU) data protection legal framework.[2]

The EC Communication provides an excellent analysis of the key challenges in developing an improved data protection legal framework. We take this opportunity to provide the EC with comments on several of the key concepts discussed in the EC Communication.

These comments build on the ongoing communication between FTC staff and the EC. Over the past year, FTC staff and Directorate-General Justice (DG Justice) have engaged in an ongoing dialogue on the processes underway in their respective jurisdictions to examine how privacy frameworks might be improved in light of a variety of impacting factors, including new and emerging technologies, and a globalized economy.

In July 2010, EC Vice President Viviane Reding (EU Commissioner for Justice, Fundamental Rights and Citizenship) and the Director-General for Justice, Françoise Le Bail, visited the FTC and met with FTC Commissioner Edith Ramirez, Bureau of Consumer Protection Director David Vladeck, and other FTC staff. We appreciate the EC's engagement with the FTC, both at senior and at staff levels, and we look forward to strengthening the relationship in the years to come.

FTC staff has submitted written comments to the EC on several privacy and data security-related subjects, including the privacy implications of Radio Frequency Identification (RFID) and proposed amendments to the EC telecommunications framework.[3] In addition, FTC staff has participated in various conferences and workshops organized by the EC.

---

[1] These comments represent the views of the staff of the Federal Trade Commission, and not necessarily the views of the Federal Trade Commission itself or any individual FTC commissioner.

[2] *Brussels, 4.11.2010, COM(2010) 609 final, available at* http://ec.europa.eu/justice/news/consulting_public/0006/com_2010_609_en.pdf.

[3] *U.S. Federal Trade Commission Staff Comments to the European Commission on its Draft Recommendation on the implementation of privacy, data protection and information security principles in applications supported by Radio Frequency Identification (RFID)* (April 2008), *available at* http://www.ftc.gov/oia/commentsrfid.pdf and *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), *available at* http://www.ftc.gov/oia/0612regulatorystafcomments.pdf.

Similarly, FTC staff benefitted from EC staff expertise on privacy and data security topics through EC staff's participation in FTC workshops and conferences. In particular, we note that an EC official participated in one of the FTC's 2010 privacy roundtables, and in previous years, other EC officials participated in FTC events.[4]

II. Background on FTC Privacy Initiatives

Privacy is one of the FTC's highest priorities. Through vigorous law enforcement, consumer and business education, and policy initiatives, the FTC devotes considerable resources to protecting the personal information of consumers. The FTC also participates in international privacy-related activities.

Since 2001, the FTC has used its authority under the FTC Act and other laws to bring 29 cases against businesses that allegedly failed to protect consumers' personal information.[5] In addition, the FTC brought numerous cases against companies that misrepresented how they collected and shared consumer information.[6]

The FTC also brought 96 cases involving unwanted spam,[7] 15 spyware cases,[8] and 15 cases against companies that violated the Children's Online Privacy Protection Act (COPPA) by collecting personal information from children under age 13 without parental consent.[9] In

---

[4] Hana Pecháčková, a policy officer in the Data Protection Unit at DG-Justice participated in the January 28, 2010 FTC Privacy Roundtable that took place in Berkeley, California. *See* agenda, *available at* http://www.ftc.gov/bcp/workshops/privacyroundtables/PrivacyRoundtables-Agenda_1-28-10.pdf.

[5] *See Privacy Initiatives, Enforcement*, FTC, http://www.ftc.gov/privacy/privacyinitiatives/promises_enf.html.

[6] *See, e.g.*, *In re GeoCities, Inc.*, 127 F.T.C. 94 (1999) (consent order) (settling charges that website had misrepresented the purposes for which it was collecting personally identifiable information from children and adults); *FTC v. Toysmart.com*, *LLC*, No. 00-11341-RGS, 2000 WL 34016434 (D. Mass. July 21, 2000) (consent order) (challenging website's attempts to sell children's personal information, despite a promise in its privacy policy that such information would never be disclosed); *see also In re Liberty Fin. Cos.*, 128 F.T.C. 240 (1999) (consent order) (alleging that site falsely represented that personal information collected from children, including information about family finances, would be maintained anonymously); *FTC v. ReverseAuction.com Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000), http://www.ftc.gov/os/2000/01/reverseconsent.htm (consent order) (settling charges that an online auction site allegedly obtained consumers' personal identifying information from a competitor site and then sent deceptive, unsolicited email messages to those consumers seeking their business); *FTC v. Sandra Rennert,* No. CV-S-00-0861-JBR (D. Nev. July 6, 2000), http://www.ftc.gov/os/caselist/9923245/9923245.shtm (consent order) (alleging that defendants misrepresented the security and encryption used to protect consumers' information and used the information in a manner contrary to their stated purpose); and *In the Matter of Educational Research Center Of America, Inc., et al.,* 135 F.T.C. 578 (2003) (consent order) (alleging that organizations failed to disclose that it shared student information for marketing purposes).

[7] *See Spam Introduction,* FTC, http://www.ftc.gov/bcp/edu/microsites/spam/index.html.

[8] *See Spyware Enforcement Actions,* FTC, http://www.ftc.gov/bcp/edu/microsites/spyware/law_enfor.htm.

[9] *See Children's Privacy Enforcement*, FTC, http://www.ftc.gov/privacy/privacyinitiatives/childrens_enf.html.

addition, the FTC has brought 64 cases involving the Do Not Call provisions of the Telemarketing Sales Rule—regulations relating to deceptive and abusive telemarketing practices.[10]

In the area of consumer and business education, the FTC uses both traditional and cutting edge means to effectively educate consumers and businesses on privacy and data security issues. FTC staff has hosted many conferences on a number of privacy-related topics, including behavioral advertising, RFID, e-commerce, mobile marketing, and children's privacy. It has also issued reports on many of these topics, in certain cases, making staff recommendations on how consumer privacy can be better protected.[11]

The FTC contributes, on behalf of the United States, to the privacy work within the Organisation for Economic Cooperation and Development (OECD) and the Asia Pacific Economic Cooperation (APEC) forum. The FTC, along with a number of foreign counterparts, including several in the EU, also recently launched a network dedicated to facilitating international enforcement cooperation in the privacy and data security areas. This network, the Global Privacy Enforcement Network (GPEN), officially launched in March 2010 and now has 22 member authorities.[12] More recently, in September 2010, the FTC was accredited as a member of Asia-Pacific Privacy Authorities forum. In October 2010, the FTC was accredited as a member of the International Conference of Data Protection and Privacy Commissioners.

III. FTC Privacy Roundtables and Report

In December 2009, the FTC hosted the first of its three roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices. Two additional roundtables took place in January and March of 2010. On December 1, 2010, the FTC staff issued a preliminary report that builds on the themes that emerged at the three roundtables and proposes a framework capable of protecting the privacy interests of consumers while also permitting innovation that relies on consumer information to develop beneficial new products and services ("FTC Report").[13] The FTC Report requests public comment on the proposals made, and the FTC staff expects to issue another report in 2011.

---

[10] 16 C.F.R. Part 310. *See also Do Not Call Enforcement Action Announcements,* FTC, http://www.ftc.gov/bcp/edu/microsites/donotcall/cases.html.

[11] For example, in a report relating to behavioral advertising, the FTC staff put forth self-regulatory principles for industry. FTC Staff, *FTC Staff Report: Self-Regulatory Principles for Online Behavioral Advertising (2009), available at* http://www.ftc.gov/os/2009/02/P0085400behavadreport.pdf.

[12] *See* www.privacyenforcement.net.

[13] FTC Staff, *Preliminary FTC Staff Report: Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers* (2010), *available at* http://www.ftc.gov/os/2010/12/101201privacyreport.pdf

In developing this proposed framework, we recognize the importance of working toward more consistent global protections for consumers and rules for business. Both the FTC Report and the EC Communication share a number of the same important concepts in considering an improved privacy framework. However, significant differences still remain, in particular, the approaches to cross-border transfers.

This comment provides input on the following key concepts discussed in the EC Communication: (a) transparency; (b) breach notification; (c) privacy by design; (d) access; (e) raising awareness; (f) adequacy; (g) global standards; and (h) enforcement and cooperation. We welcome the opportunity to discuss these with you in further detail.

IV. **Key Concepts**

A. Transparency. The EC Communication states that the EC will consider a general principle of "transparent processing of personal data" in the improved legal framework, and that this may include specific obligations with respect to the type of information to be provided and the "modalities" for providing such information. The EC Communication further states that the EC will consider drawing up one or more EU standard "privacy information notices" to be used by data controllers.[14]

FTC staff agrees with the EC that greater transparency is essential in an improved privacy framework. The FTC Report points out that many data practices are invisible to consumers.[15] Our report therefore encourages companies to implement a number of measures to make their data practices more transparent to consumers. For example, one measure discussed in the FTC Report is the need to simplify consumer choice and to provide choice mechanisms in a prominent, relevant, and easily accessible place for consumers.[16]

One method of simplified choice discussed in the FTC Report is a "Do Not Track" mechanism governing the collection of information about consumer's Internet activity to deliver targeted advertisements and for other purposes. Consumers and industry both support increased transparency and choice for this largely invisible practice. The FTC recommends a simple, easy to use choice mechanism for consumers to opt out of the collection of information about their Internet behavior for targeted ads. The most practical method would probably involve the placement of a persistent setting, similar to a cookie, on the consumer's browser signaling the consumer's choices about being tracked and receiving targeted ads. We note that a recent European Parliament resolution has similarly voiced concern about behavioral advertising. We

[14] EC Communication at 6.

[15] "[C]onsumers are generally unaware of the number of online and offline entities that collect their data, the breadth of the data collected, and the extent to which data is shared with third parties that are often entirely unknown to consumers." FTC Report at 42.

[16] FTC Report at 52-69.

welcome the opportunity to discuss with the EC how it plans to proceed with respect to the concerns raised in that resolution.[17]

In addition, we would like to learn more from the EC staff about what is being contemplated with regard to the "EU standard forms." Like the EC Communication, the FTC Report also discusses the use of standard terms in notices presented to consumers. This standardization might enable consumers to more easily compare companies' business practices. The FTC Report requests comments from stakeholders on the feasibility of standardizing the format of notices and the terminology used in disclosures.[18]

B. Breach notification. The EC Communication states that the EC will examine the introduction of a general breach notification requirement, including who must be given notice of such a breach and the threshold criteria that would trigger the notice obligation.[19] The EC Communication points out that in the current EU legal framework, the breach notification obligation is limited to the telecommunications sector.

FTC staff believes that breach notification obligations should not be limited to any one sector. Breach notification, a legal obligation developed in the United States, is now required in more than 45 of the individual states in the United States.[20] The FTC continues to advocate for federal breach notification legislation, not limited to specific sectors.[21] Currently, on the federal level, breach notification is required only in certain areas (for example, health information, and information held by financial institutions), and only in specified circumstances.[22]

---

[17] *See* http://www.europarl.europa.eu/sides/getDoc.do?type=TA&language=EN&reference=P7-TA-2010-0484.

[18] FTC Report at 70-72.

[19] EC Communication at 7.

[20] *See* list of state breach notification laws posted by the National Conference of State Legislatures, *available at* http://www.ncsl.org/default.aspx?tabid=13489.

[21] *See, e.g., Data Security: Hearing Before The Subcommittee On Consumer Protection, Product Safety, and Insurance of the Senate Committee on Commerce, Science, and Transportation* 111th Cong. (Sept. 22, 2010) at 11, *available at* http://www.ftc.gov/os/testimony/100922datasecuritytestimony.pdf (prepared statement of the FTC).

[22] The FTC and the Department of Health and Human Services enforce health information breach notification rules. S*ee* Health Breach Notification Rule, 16 C.F.R. 318, *available at* http://www.ftc.gov/os/2009/08/R911002hbn.pdf, and Subpart D—Notification in the Case of Breach of Unsecured Protected Health Information, 45 C.F.R. Part 164.400, *available at* http://edocket.access.gpo.gov/2009/pdf/E9-20169.pdf. Guidance issued by U.S. federal banking regulators in connection with the Gramm-Leach-Bliley Act, 15 U.S.C. §§ 6801-6809 (2010), contains customer notification procedures in the event 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, Part III of Supplement A to Appendix B, at 12 C.F.R. Part 30 (Office of the Comptroller of the Currency), Supplement A to Appendix D-2, at 12 C.F.R. Part 208 (Federal Reserve System), 12 C.F.R. Part 364 (Federal Deposit Insurance Corporation), and 12 C.F.R. Part 568 (Office of Thrift Supervision), 70 Fed. Reg. 15736 - 15754 (March 29, 2005).

We note that in 2006, when the EC was considering changes to the EU regulatory framework for electronic communications networks and services, FTC staff submitted a comment to the EC advocating that breach notification not be limited to the telecommunications sector.[23]

C. Privacy by Design. The EC Communication indicates that the EC will examine how the concept of "Privacy by Design" can improve compliance with data protection rules.[24] We note that in the FTC Report, we recommend that companies adopt a "Privacy by Design" approach.[25] This would involve building privacy protections into everyday business practices. These protections would include providing reasonable security for personal information, collecting only the data necessary for a specific business purpose, and retaining data only for the period of time required to fulfill that purpose.

The FTC Report further notes that the implementation of "Privacy by Design" within industry can be scaled to each company's business operations.[26] This takes into account company differences, including size, amount of personal information collected, and type of personal information collected. We would welcome the opportunity to discuss the concept of "Privacy by Design" with the EC and whether scalability is being considered in connection with possible "Privacy by Design" requirements in the revised EU data protection framework.

D. Access. The EC Communication notes that the current EU framework provides consumers with rights to access the information being held about them, along with the right to have that information corrected or deleted. The EC Communication also notes, however, that these rights are not harmonized within the EU Member States, and that access has become particularly challenging in connection with the online environment. The EC Communication therefore states that the rights of consumers in connection with access should be made more explicit and possibly strengthened.

The FTC Report proposes providing consumers with reasonable access to the data that companies maintain about them, particularly for companies that do not interact with consumers directly, such as data brokers. We are mindful, however, of the significant costs associated with access. Accordingly, we suggest that the extent of access should be proportional to both the sensitivity of the data and its intended use.[27]

---

[23] *See* note 3 *supra.*

[24] EC Communication at 12.

[25] FTC Report at 41.

[26] FTC Report at v.

[27] FTC Report at 72-76.

The FTC Report raises a number of questions relating to access, and we are seeking comment on these issues. Among the questions are: (a) whether companies should be able to charge a reasonable cost for certain types of access; (b) whether companies should be required to inform consumers of the identity of those with whom the company has shared data about the consumer, as well as how they obtained the data; and (c) whether access to data should differ for consumer-facing and non-consumer-facing entities.

We welcome the opportunity to learn more from the EU experience with regard to legal requirements to provide access to consumers, and what consideration the EC has given to a proportional approach of the sort discussed in the FTC Report.

We also would like to learn about the extent to which EU consumers are aware of their access rights, the extent to which these rights are exercised,[28] and any burdens that providing access imposes.

E. Raising Awareness. The EC Communication stresses the importance of making consumers more aware of the risks of sharing their personal information, and of the legal protections in place for their personal information. We also note that the EC Communication calls for a broad range of stakeholders to engage in awareness-raising activities, including data protection authorities, industry, educational institutions and civil society.

In the FTC Report, we also explore the important issue of educating consumers, as well as businesses. The FTC Report poses a number of questions for comment, including:

> *How can individual businesses, industry associations, consumer groups and government do a better job of informing consumers about privacy?*
>
> *What role should government and industry associations have in educating businesses?*[29]

It is evident that the EC and the FTC both place a high priority on education and we believe it would be useful to share experiences on how we can improve consumer awareness of these issues globally.

F. Adequacy. The EC Communication, in discussing how "adequacy assessments" are conducted, indicates that, among other things, the EC intends to "clarify the Commission's adequacy procedure and better specify the criteria and requirements for assessing the level of data protection in a third country or an international organization."[30]

---

[28] We note that a 2008 Flash Eurobarometer indicated that only 59% of those surveyed were aware that they had the right to access the personal data held about them by organizations. *See* Flash Eurobarometer Series #225 Data Protection in the European Union - Citizens' Perceptions (2008) at 26, *available at* http://ec.europa.eu/public_opinion/flash/fl_225_en.pdf. We would be interested in any further available information on this subject.

[29] FTC Report at A-6.

[30] EC Communication at 16.

The EC Communication identifies certain difficulties with "adequacy," including the lack of harmonization among the Member States. While the lack of harmonization may indeed be a challenge, additional significant shortcomings in the "adequacy" framework are the lack of clarity in the procedure and the cumbersome nature of the process. Research suggests that in the EU, "rules on data export and transfer to third countries are outmoded," and that "the tools providing for transfer to third countries are cumbersome."[31]

The "adequacy" approach focuses on the legal framework of the jurisdiction where the data recipient is located, and not on the data protection practices of the actual data recipient. Indeed, it seems that only if data is transferred pursuant to one of the mechanisms developed pursuant to Article 26(2) of the Data Protection Directive [32] (*e.g.*, binding corporate rules or model contract clauses), is the recipient required to disclose how it protects personal information. If the recipient is within the EU or in a country deemed "adequate," then the data controller can export the data without the recipient having to disclose information about their information handling practices, or ever having agreed to treat the information in an appropriate manner.

We welcome the opportunity to discuss with the EC how to move towards more transparent frameworks that better protect the privacy of individuals' personal data. The FTC is currently involved in the privacy-related work of the Asia Pacific Economic Cooperation (APEC), where efforts are underway to develop more workable mechanisms relating to the cross-border transfer of data.[33]

G. Global Standards. The EC Communication states that the EC will "continue to promote the development of high level and technical standards of data protection in third countries and at international level."

With regard to international standards, data protection and privacy is a highly complex and technical subject in which there remain significant unresolved political and policy debates. Indeed, both the FTC and the EC are in the process of reviewing their respective legal frameworks. We also point out that the United Nations' International Law Commission has commented that data protection is an area "in which State practice is not yet extensive or fully developed."[34]

---

[31] See Review of the European Data Protection Directive, Rand Europe (2009) at 33-34, available at http://www.rand.org/content/dam/rand/pubs/technical_reports/2009/RAND_TR710.pdf.

[32] Directive 95/46/EC of the European Parliament and of the Council of 24.10.1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

[33] *See* http://www.apec.org/en/Groups/Committee-on-Trade-and-Investment/Electronic-Commerce-Steering-Group.aspx.

[34] U.N. International Law Commission (ILC), "Report on the Work of its Fifty-Eighth Session" (1 May to 9 June to 11 August 2006) U.N. Doc A/61/10, 499, available at http://untreaty.un.org/ilc/reports/2006/2006report.htm.

Given the lack of consensus in this area, we support efforts to promote more consistency and inter-operability. However, we suggest that binding general international standards at this stage are premature. Differing cultures and values result in different approaches among jurisdictions. For example, enforcement priorities, regulation, the role of self-regulation, labor rights, property holder rights, litigation discovery and trial rules, choice of law, judgment recognition, views on the proper role of government, and freedom of expression are all important interests—some of constitutional dimensions in many jurisdictions—that affect how data privacy is approached.[35]

We agree that continued international engagement and dialogue on more consistent privacy protections and rules for businesses is essential. At this stage, however, we suggest that rather than focusing on substantive rules, the primary focus should be on the development of an appropriate procedural framework for considering how a global standard might be developed, based on input from all international regions and stakeholders, including those that are currently still in the process of rethinking, modernizing and establishing their regional privacy approaches.

FTC staff previously stressed the importance of such a process in its comments on the International Conference of Data Protection and Privacy Commissioner's *Joint Proposal for International Standards on the Protection Of Privacy With Regard to the Processing Of Personal Data.*[36] In our August 2010 comments on the Joint Proposal, which we prepared jointly with the Privacy Office of the U.S. Department of Homeland Security, we recommended that "all relevant stakeholders in the international privacy dialogue collaborate and develop a meaningful way to achieve broader input on the feasibility of an international data privacy standard."[37]

H. Enforcement and Cooperation. The EC Communication notes the current limitations on the enforcement powers and practices of the data protection authorities, and the importance of the availability of effective remedies and sanctions.

---

[35] Illustrations of jurisdictions balancing such rights with privacy include several cases from the European Court of Justice. *See*, e.g., Case C-101/01 Criminal Proceedings against Bodil Lindqvist (European Court of Justice, November 6, 2003), available at http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?lang=en&num=79968893C19010101&doc=T&ouvert=T&seance=ARRET (Court ruled that when applying national legislation implementing Directive 95/46, it is the role of the Member State authorities and courts to ensure a "fair balance between the rights and interests in question," including freedom of expression), and Case C-275/06 *Productores de Música de España (Promusicae) v Telefónica de España SAU* (European Court of Justice, January 29, 2008), available at http://curia.europa.eu/jurisp/cgi-bin/gettext.pl?where=&lang=en&num=79919870C19060275&doc=T&ouvert=T&seance=ARRET (Court ruled that when transposing directives on intellectual property and data protection, Member States must consider how to strike a "fair balance" between the fundamental rights protected by the European Community legal order).

[36]The Join Proposal is available at http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf

[37] *See* http://www.ftc.gov/os/2010/08/100810madridcomments.pdf at 1-4.

While policy initiatives are an important priority for the FTC, we believe that enforcement is the most essential element of an effective privacy framework. The FTC will continue to vigorously enforce in the areas of privacy and data security.

In a global economy, there is universal recognition that international enforcement cooperation is essential in the privacy area. Accordingly, a network such as GPEN that facilitates such cooperation is increasingly essential. The EC Communication advocates for better enforcement cooperation among the Member State data protection authorities. We encourage stressing the importance of such enforcement cooperation not only within the EU, but also internationally. Enforcement cooperation is not without challenges. For example, developing frameworks for the exchange of information—a necessary part of cooperation on specific enforcement matters—may present certain challenges. We encourage the EC to consider how it can facilitate the cooperation of the Member State DPAs with their international counterparts.

* * *

We very much appreciate the opportunity to provide these comments and would welcome the opportunity to discuss these issues further. Any questions or comments can be directed to Hugh Stevenson, Deputy Director, Office of International Affairs at the U.S. Federal Trade Commission, hstevenson@ftc.gov, 202-326-3511, or to Yael Weinman, Counsel for International Consumer Protection, Office of International Affairs at the U.S. Federal Trade Commission yweinman@ftc.gov, 202-326-3748. Thank you.