U.S. Federal Trade Commission Staff Comments to the Council of Europe's Consultative Committee on the Modernization of Convention 108[1]

March 9, 2011

I. Introduction

United States Federal Trade Commission (FTC) staff submits the following comments to the Council of Europe's Consultative Committee in response to its request for comments on modernizing the 1981 Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data and its 2001 Protocol regarding supervisory authorities and transborder data flows ("Convention 108").

The FTC staff commends the Consultative Committee on undertaking this review, and for raising many critical questions in contemplating this modernization, as set forth in the Consultative Committee's consultation paper requesting comments.[2] The consultation paper raises a broad array of very complex questions, and given time constraints we cannot address all the relevant ones here. Moreover, we are mindful that we submit our comments as outside observers; the United States is of course not a party to Convention 108. Instead, we offer at this time comments on a few of the key issues raised, and some background on our own consultation process on many similar issues.

As the Consultative Committee is aware, the European Commission (EC) is also considering how to improve the privacy framework in the European Union (EU). The Organization for Economic Cooperation and Development (OECD) is also examining the 1980 OECD Privacy Guidelines, and as described below, the FTC has also undertaken a wide-ranging initiative to consider how the U.S. privacy framework might be improved. We believe there is great value in continuing the dialogue among the various bodies examining privacy frameworks. The FTC participates in the OECD committee examining the 1980 Privacy Guidelines, and has taken several opportunities to engage with the European Commission on its work developing an improved privacy framework in the EU.[3] We appreciated the opportunity for FTC staff and FTC Commissioner Julie Brill to meet with the Council of Europe's Deputy Secretary General Maud de Boer-Buquicchio last week, and we welcome further occasions to exchange views on these issues.

II. FTC Examination

For more than a year, the FTC has been re-examining the privacy framework now used in the United States. In December 2009, the FTC hosted the first of three roundtables to explore the privacy issues and challenges associated with 21st century technology and business practices.

---

[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] *Available at* http://www.coe.int/t/dghl/standardsetting/dataprotection/Consultation_Modernisation_Convention_108_EN.pdf.

[3] The FTC staff submitted comments to the European Commission (EC) in connection with the EC consultation. These comments, submitted on January 13, 2011, are *available at* http://www.ftc.gov/os/2011/01/111301dataprotectframework.pdf

We organized two additional roundtables in January and March of 2010. On December 1, 2010, FTC staff issued a 122-page preliminary report that builds on the themes that emerged at the three roundtables, and that proposes a framework capable of protecting the privacy interests of consumers while also permitting the use of consumer information to develop beneficial new products and services ("FTC Report").[4] We think you will find considerable material in the FTC Report that addresses the issues raised in your consultation process.

We also note that the U.S. Department of Commerce issued a paper on December 16, 2010, containing policy recommendations in the privacy area—*Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*.[5] This paper is the result of a U.S. Department of Commerce public consultation initiative.

The FTC Report makes a number of recommendations, including the following: (a) companies should adopt a "privacy by design" approach by building privacy protections into their everyday business practices; (b) consumers should be presented with choice about collection and sharing of their data at the time and in the context in which they are making decisions about the collection or use of their data; and (c) information practices should be more transparent to consumers and consumers should be allowed reasonable access to the data companies maintain about them, particularly for non-consumer facing entities such as data brokers.

The FTC Report also suggests implementation of a "Do Not Track" mechanism for online behavioral advertising – likely a persistent setting on consumers' browsers – so consumers can choose whether to allow the companies to collect information about them as they browse the web.

The FTC Report requested comment on the proposals made; we received more than 400 comments, including some from foreign counterparts. We expect that FTC staff will issue another report later this year that takes into account the input received in these numerous comments.

III. Consultative Committee Consultation Paper

The Consultative Committee Consultation Paper raises a number of issues and questions in considering modernizing Convention 108. We take this opportunity to provide the Consultative Committee with input on several of the issues and questions raised in the Consultation Paper.

A. Consent.

The Consultation Paper asks:

---

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

[5] *Available at* http://www.ntia.doc.gov/reports/2010/IPTF_Privacy_GreenPaper_12162010.pdf

Should the question of consent be considered, in close connection with the principle of transparency and obligation to inform, or as a necessary condition to a fair and lawful processing, to satisfy before any other step?

The FTC Report emphasizes that greater transparency is essential in an improved privacy framework. The FTC Report points out that many data practices are invisible to consumers, and therefore we encourage companies to implement a number of measures to make their data practices more transparent to consumers.[6] For example, one idea 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.[7]

Having said that, the FTC Report also suggests that for commonly accepted practices, choice should not be necessary; eliminating choices for practices obvious to consumers would make the choices for practices of greater concern more meaningful.[8] For example, consumers are aware that their information would be provided to the shipper to fulfill an online order—mandating choice for this use distracts consumers from the choices they need to make in other areas, for example disclosure of their information to third parties unrelated to order fulfillment. Thus, we encourage the Consultative Committee to consider the question of consent taking into account commonly accepted practices where consent may not be necessary.

B. Children.

The Consultation Paper raises the following points:

A specific protection could also be applied to certain categories of data subjects. In particular, children may need specific protection because of their vulnerability. Is there a need for specific provisions regarding the protection of children? If so, which are the issues that should be addressed in such provisions?

We note that in the United States, a specialized statute governs children's online privacy. This statue, the Children's Online Privacy Protection Act (COPPA)[9] requires that the FTC issue and enforce a rule protecting children's online privacy. This Rule went into effect in April 2000.[10] We believe that there are unique issues relating to the online privacy of children, and formulating a specialized rule has been useful in this area.

The primary goal of the COPPA statute and Rule is to put parents in control over what information is collected from their children online. The Rule was designed to protect children

[6] "[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.

[7] FTC Report at 52-69.

[8] FTC Report at 53-57.

[9] 15 U.S.C. §§ 6501-6506.

[10] 16 C.F.R. Part 312.

under age 13 while accounting for the dynamic nature of the Internet. The Rule applies to operators of commercial websites and online services directed to children under 13 that collect, use, or disclose personal information from children, and operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. Businesses covered by the Rule must:

1. Post a clear and comprehensive privacy policy on their website describing their information practices for children's personal information;

2. Provide direct notice to parents and obtain verifiable parental consent, with limited exceptions, before collecting personal information from children;

3. Give parents the choice of consenting to the operator's collection and internal use of a child's information, but prohibiting the operator from disclosing that information to third parties;

4. Provide parents access to their child's personal information to review and/or have the information deleted;

5. Give parents the opportunity to prevent further use or online collection of a child's personal information;

6. Maintain the confidentiality, security, and integrity of information they collect from children.

In addition, the Rule prohibits operators from conditioning a child's participation in an online activity on the child's providing more information than is reasonably necessary to participate in that activity.

It has been nearly eleven years since the Rule went into effect. In light of the rapid-fire pace of technological developments in recent years, including an explosion in children's use of mobile devices and interactive gaming, the FTC accelerated its review of COPPA to make sure that it is still adequately protecting children's privacy. The review was earlier scheduled to take place in 2015, but the FTC accelerated this process and in March 2010, sought comments on revising the Rule.[11] In addition, in June 2010, the FTC hosted a public roundtable on issues relating to the Rule.[12] FTC staff is currently reviewing comments received from a broad range of stakeholders and is considering whether there is a need for any modifications to the Rule.

C. Data Security

The Consultation Paper asks:

[11] Request for Public Comment on the Federal Trade Commission's Implementation of the Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2010), *available at* http://www.ftc.gov/os/fedreg/2010/april/P104503coppa-rule.pdf.

[12] http://www.ftc.gov/bcp/workshops/coppa/index.shtml.

Article 7 of the Convention addresses security in a narrow sense, namely as protection against accidental or unauthorised destruction, accidental loss and unauthorised access, alteration or dissemination. Should the notion of security also include a right for data subjects to be informed of data security breaches?

The FTC believes that data breach notification in appropriate circumstances is beneficial. In the United States, many of the individual states have passed breach notification laws and some also have imposed data security requirements on companies operating within their states. These laws have further increased public awareness of data security issues and related harms, as well as data security issues at specific companies. The FTC has been advocating for breach notification legislation at the federal level in order to extend notification nationwide. We note that one of the most important considerations in contemplating breach notification is determining the thresholds that would trigger the notification requirement. It may not be appropriate to require notification in all circumstances—certain factors should be taken into account, including the extent of the breach and the likelihood of injury. Requiring notification in every situation may distract consumers from those breaches that are of the greatest concern.

D. Accountability.

The Consultative Committee Consultation paper asks:

Should accountability mechanisms and an obligation to demonstrate that effective measures have been taken in order to ensure full respect of data protection rules be introduced?

We encourage the development of mechanisms that would enable companies to demonstrate compliance with laws, regulations, self-regulatory codes of conduct, or their own internal policies and procedures. As discussed in more detail in paragraph III.G, below, an effort to promote greater accountability in the privacy area, through the development of cross-border privacy rules, is underway within the Asia-Pacific region through the work of the Asia-Pacific Economic Cooperation (APEC) forum. Such an accountability mechanism holds great promise, both domestically, and in the area of cross-border data transfers, and we encourage dialogue within the international privacy community to consider how to develop additional mechanisms.

E. Privacy by Design.

The Consultative Committee Consultation paper asks:

Should the principle of privacy by design, which aims at addressing data protection concerns at the stage of conception of a product, service, or information system, be introduced?

In the FTC Report, we recommend that companies adopt a "Privacy by Design" approach.[13] This would involve building privacy protections into everyday business practices. These protections would include providing reasonable security for personal information,

[13] FTC Report at 41.

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.[14] This takes into account company differences, including size, amount of personal information collected, and type of personal information collected. We would encourage the Consultative Committee to consider the important concept of scalability in considering the issue of Privacy by Design.

F. Access. The Consultative Committee Consultation Paper asks:

> *The right of access should not be limited to data but should cover access to the origin of the data, i.e. who was at the origin of the communication. Should this right also cover access to the logic of the processing?*

We are unclear on what is meant by the "access to the logic" of the processing of the data and would appreciate clarification on this point. Perhaps this refers to providing individuals with the company's reasoning with regard to certain decisions made impacting consumers. We note that in the United States, consumers have a right to be informed if certain companies take an action that has a negative impact on the consumer, if such action was based at least in part on information contained in the consumer's credit report. In such event, consumers would also have the right to obtain a copy of their credit report. An example of an action having a negative impact (the term used in U.S. law is "adverse action") includes the denial or cancellation of credit or insurance, or the denying of employment or promotion.[15] Consumers also have a right to obtain a credit score, generally for a small fee.[16] While credit reporting agencies are not required to reveal precisely how credit scores are calculated, the disclosure must include the range of possible credit scores in the scoring model and key factors that adversely affected the consumer's score.[17]

We note that 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.[18]

The FTC Report raises a number of questions relating to access, and we specifically sought 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

[14] FTC Report at v.

[15] 15 U.S.C. 1681m(a).

[16] 15 U.S.C. 1681g(f).

[17] *Id.*

[18] FTC Report at 72-76.

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 would be interested in learning more about the Consultative Committee's rationale in determining that access rights should include the origin of the information that a company has about an individual—as noted above, that is one of the questions posed in the FTC Report.

G. Free Flow of Information.

The Consultative Committee Consultation Paper asks:

> *Do we need to reconsider the notion of "transborder data flows" altogether in the Internet age, where data instantaneously flows across borders? Would it be useful to establish internationally agreed minimum rules to ensure cross-border privacy? What could be their content?*

We note that like the EU Data Protection Directive, the Additional Protocol to Convention 108 contains an "adequacy" provision. 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. As we have noted in our comments to the European Commission, significant shortcomings in the "adequacy" framework include 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."[19] The process appears if anything more complex for countries applying both the EU and the Convention 108 adequacy standards. This suggests that there may be value in reconsidering the Convention 108 "adequacy" requirement, and also in considering the impact of having data flow restrictions in two different regional legal instruments with overlapping signatories.

The FTC is currently involved in the privacy-related work of APEC, where efforts are underway to develop more workable mechanisms relating to the cross-border transfer of data.[20] In particular, we have been working on the development of the APEC cross-border privacy rules system. This is a reciprocal program governing cross-border information transfers among companies in the APEC region. Once the system is operational, we believe that it has tremendous potential to facilitate accountable and efficient data transfers within the APEC region. All stakeholders in such a system could benefit significantly—consumers because they are dealing with accountable organizations who have opted into an efficient privacy management system that includes effective complaint resolution procedures; companies because the system creates greater efficiency, uniformity and predictability with respect to their privacy and data security requirements; and privacy enforcement authorities such as the FTC, because an efficient self-regulatory system, coupled with effective backstop enforcement contingencies, improves the effectiveness of their privacy enforcement missions.

---

[19] 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

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

With regard to internationally agreed-upon privacy rules, we believe that at this stage, 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*.[21] 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."[22]

Data protection and privacy are highly complex and technical subjects in which there remain significant unresolved political and policy debates. Indeed, the United States, the European Commission, and the OECD are also in the process of reviewing their respective 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."[23]

* * *

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.

[21] The English language version of the *Joint Proposal* is available on the website of the Spanish data protection authority, at http://www.agpd.es/portalwebAGPD/canaldocumentacion/conferencias/common/pdfs/31_conferencia_internacional/estandares_resolucion_madrid_en.pdf.

[22] The FTC staff and DHS Privacy Office August 2010 comment is *available at* http://www.ftc.gov/os/2010/08/100810madridcomments.pdf

[23] 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.