COMMENTS BY THE DHS PRIVACY OFFICE AND THE STAFF OF THE U.S. FEDERAL TRADE COMMISSION ON THE JOINT PROPOSAL FOR INTERNATIONAL STANDARDS ON THE PROTECTION OF PRIVACY WITH REGARD TO THE PROCESSING OF PERSONAL DATA

August 10, 2010

These comments are submitted by the United States Federal Trade Commission ("FTC") staff and the United States Department of Homeland Security Privacy Office ("DHS Privacy Office") on the Joint Proposal for International Standards on the Protection of Privacy with Regard to the Processing of Personal Data ("Madrid Resolution").[1]

Staff from these agencies had the opportunity to participate in the experts' meetings organized by the International Conference of Data Protection and Privacy Commissioners (ICDPPC) that took place in Barcelona in January 2009 and in Bilbao in June 2009 during which the development of the Madrid Resolution was discussed. Comments on a draft version of the Madrid Resolution were previously submitted by FTC staff and the DHS Privacy Office to the ICDPPC in May 2009.[2]

Staff from these two U.S. agencies also attended the ICDPPC conference in Madrid in November 2009 as observers. In Madrid, the final text of the Madrid Resolution was unveiled.[3] Not having had the opportunity to review this text prior to Madrid, the FTC staff and the DHS Privacy Office now take this opportunity to provide their input. We would welcome the opportunity to engage in further discussion with the ICDPPC and other stakeholders on the points raised below.

1. Scope and Process

Data privacy is a highly complex and technical subject in which there remain significant unresolved political and policy debates. The United Nations' International Law Commission has noted that data protection is an area "in which State practice is not yet extensive or fully developed."[4]

---

[1] These comments do not necessarily represent an official position of the United States Government; rather, they represent the views of the DHS Privacy Office and Federal Trade Commission staff.

[2] These comments are available at *http://www.ftc.gov/oia/dhscomments.pdf*.

[3] The final text of the Madrid Resolution was not provided to the FTC or DHS in advance of the Madrid meeting, nor was it accompanied by an explanation as why changes were made to earlier drafts. Thus, we are unaware what review process for this text may have taken place within the ICDPPC, an organization of which neither DHS nor FTC is a member.

[4] 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.

At the outset, we note that international conventions typically cover a narrow issue with broad consensus. The Madrid Resolution covers an extremely broad array of issues with which there is narrow consensus. The limits on current consensus appear to add to the challenge of developing a standard in this area.

In fact, a number of jurisdictions lack data privacy frameworks, while others are currently rethinking the frameworks that are in place. For example, in the United States, the FTC recently conducted a series of public roundtable discussions to examine, among other things, the effectiveness of the existing U.S. legal and self-regulatory regimes to address consumer privacy interests. The FTC is now in the process of reviewing these discussions, along with the many submissions it received from a variety of stakeholders in connection with this initiative.[5] The U.S. Department of Commerce is also conducting a comprehensive review of the nexus between privacy policy and innovation in the Internet economy and recently held a symposium in May 2010 to explore this topic in depth.[6] In the European Union, the European Commission is now evaluating the information it gathered in response to its 2009 consultation aimed to "obtain views on the new challenges for personal data protection in order to maintain an effective and comprehensive legal framework to protect individual's personal data within the EU."[7]

In addition, the Organization for Economic Cooperation and Development (OECD), in connection with the 30th anniversary of the 1980 OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, has planned a number of events and is preparing a report examining how the Guidelines operate in the present day. Development of a global privacy standard is therefore extremely challenging. Consideration of a standard must take these current consultations into account and the input to these consultations will be particularly useful in determining the areas of common ground as well as those that are more challenging to harmonize.

An additional challenge arises from different approaches to data privacy resulting from a country's culture and values. In fact, an earlier ICDPPC resolution states

---

[5] *See* http://www.ftc.gov/bcp/workshops/privacyroundtables/index.shtml. The FTC has posted more than 100 submissions received from a variety of stakeholders (*e.g.*, government, academic, civil society, industry, and private citizens) in connection with this initiative.

[6] *See* http://www.ntia.doc.gov/frnotices/2010/FR_PrivacyNOI_04232010.pdf, and http://www.ntia.doc.gov/internetpolicytaskforce/privacy/symposiumagenda_05072010.pdf.

[7] *See* http://ec.europa.eu/justice_home/news/consulting_public/news_consulting_0003_en.htm. The European Commission has posted more than 160 submissions to its consultation, which like the submissions made to the FTC, include a variety of stakeholders, including government, civil society, industry and private citizens.

that it "[r]ecognise[s] that countries have adopted different approaches to protecting personal information and enhancing privacy rights."[8] 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.[9] It will be difficult for an international data privacy standard to work through all these issues and develop sufficient common ground in a way that will enhance the already existing guidelines (for example, the 1980 OECD Privacy Guidelines and the APEC Privacy Framework).

Given these challenges, we see the Madrid Resolution developed by the ICDPPC as a useful starting point to begin the conversation on the feasibility of a global data privacy standard. To continue the conversation, however, it is important to have a dialogue that reaches all stakeholders. In particular, we note that the Madrid Resolution aims to apply both to the private and the public sectors. Accordingly, government authorities that use personal information to carry out their mandated functions need to be included in further dialogue in connection with the feasibility of a global data privacy standard. To date, representatives from such authorities have not been included in the discussions that led to the development of the Madrid Resolution. Because there is not a uniform approach to domestic privacy protections as to public sector functions it is imperative that these authorities be included in discussions about any global data privacy standard to the extent it covers the public sector.[10]

---

[8] ICDPPC Resolution on International Co-operation (2007), *available at* *http://www.privacyconference2007.gc.ca/Terra_Incognita_resolutions_E.html*.

[9] Illustrations of jurisdictions balancing such rights 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).

[10] We note that even within the European Union, there has not been a uniform approach. In a joint opinion dated December 2007, relating to the proposal for a Council Framework Decision on the use of Passenger Name Record (PNR) for law enforcement purposes, the Article 29 Working Party and the Working Party on Police and Justice noted that "not all Member States have included police and justice in their transposition in national law of Directive 95/46/EC." See http://ec.europa.eu/justice_home/fsj/privacy/docs/wpdocs/2007/wp145_en.pdf at p. 11. Moreover, the Lisbon Treaty may result in changes to the overall data protection framework in the EU, in particular,

We recommend 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. This broader input must go beyond those who had the opportunity to work on the development of the Madrid Resolution, which represents only regulators with privacy enforcement authority. Many countries, including the most populous ones, have not been engaged in this consultation with the ICDPPC - - the ICDPPC represents only about a tenth of the world's population. In addition, there should be greater outreach and interaction between public and private data privacy experts, and international legal experts.

2. Private and Family Life Processing

The Madrid Resolution states that national legislation may "lay down that the provisions of this Document do not apply to the processing of personal data by a natural person in the course of activities related exclusively to his/her private and family life." This text does not require States to exclude "private and family life processing," but rather leaves it to a State's discretion as to whether there should be such an exclusion. The application of data processing legal requirements to personal activities goes beyond what is currently required in existing international legal instruments. This could lead to inconsistent requirements and might present challenges to individuals with friends and relatives around the globe, which is often the norm in today's world. Indeed, the 95/46 Data Protection Directive specifically states that the Directive does not apply to the processing of personal data "by a natural person in the course of a purely personal or household activity."[11]

3. Restrictions

Section 5 of the Madrid Resolution states that countries may restrict the scope of certain provisions "when necessary in a democratic society in the interests of national security, public safety, for the protection of public health, or for the protection of the rights and freedoms of others." This will lead to inconsistent exceptions due to differing legal frameworks and cultural differences. For example, jurisdictions use different criteria to determine whether there is a freedom of expression concern or public health emergency that would warrant actions restricting the provisions in the Madrid Resolution. With regard to

---

raising the question whether and to what extent police and justice matters will be subject to the same requirements as other sectors.

[11] Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ("95/46 Data Protection Directive") Official Journal L 281 , 23/11/1995 P. 0031 – 0050, *available at* http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML.

national security, jurisdictions may make different determinations as to whether there is a credible risk to national security.

FTC staff also notes that the previous version of the Madrid Resolution provided for a restriction in the interest of "the economic well being of the country." This exclusion is not in the final draft proposal and we question why it was removed. The economic well being of a State is an important interest and it may be necessary to allow States certain discretion in the application of the provisions of the Madrid Resolution to protect this interest.

4. International Transfers

The provisions of Section 15, "International Transfers," state that international transfers are permitted to States that do not afford the level of protection consistent with the document if the transferor can guarantee that the recipient will afford such level of protection. This suggests that the Madrid Resolution is advocating a flexible approach and not advocating for an EU type "adequacy" standard. However, the text then allows individual states to require pre-approval from an authority prior to international transfers. Such a pre-approval requirement is quite burdensome and negates the flexible approach that moves away from an "adequacy" standard. Moreover, a pre-approval process would arguably absolve companies of being held accountable for ensuring that the recipient of the data is treating it appropriately in accordance with the requirements of the Madrid Resolution.

5. Access

Section 16, which discusses the "Right of Access," states that the data subject has the right to obtain "information on the specific personal data subject to processing." This text is ambiguous - - it is unclear whether the responsible person is required to turn over the actual information they hold about the data subject, or rather only the nature of the information held. For example, it is not clear whether the responsible person needs to disclose the actual address that it has for the data subject, or just the fact that it is has an address for the data subject.

6. Security

The first paragraph of Section 20 on security requires the use of appropriate standards based on the associated risks to protect personal information. We agree with this approach to security requirements.[12]

[12] Indeed, the Safeguards Rule enforced by the FTC pursuant to the Gramm-Leach-Bliley Act, (15 U.S.C. §§ 6801-6809), requires financial institutions to develop, implement, and maintain "reasonable administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information." See *http://www.ftc.gov/os/2002/05/67fr36585.pdf*.

FTC staff notes that paragraph 2 of the Section states that data breach notification would be required if it "could significantly affect their pecuniary or non-pecuniary rights." This threshold is quite broad. Legal requirements in this area are in the beginning stages, and at this point it seems difficult to find consensus on specific requirements that would apply in all situations and to all categories of personal data.

Accordingly, at this time it would seem difficult to set forth specific criteria that triggers the data breach notification requirement in all situations. Also, with regard to the requirement in the Madrid Resolution to inform data subjects of the measures taken to resolve the data breach, we note that there may be situations where the measures taken for resolution will involve cooperation with law enforcement conducting criminal investigations. In such cases, it may not be appropriate to disclose those publicly.

7. Compliance and Monitoring

The Sections discussing compliance and monitoring (Section 22-25) are overly reliant on the independent supervisory authority model. The concept of the independent supervisory authority raises many questions, even within the EU, where it is required by law. The necessary criteria to be considered an "independent" authority is not clear. In fact, the European Court of Justice recently ruled that certain of Germany's data protection authorities did not meet the "independence" criteria required by the 95/46 Data Directive because they were subject to "State scrutiny."[13] For many jurisdictions, it may be difficult to construct a fully independent authority that at the same time is an entity of the State. Any language addressing compliance and monitoring for both public and private sectors must be flexible enough to accommodate the range of democratic legal systems. Finally, it is not explained why there is a preference for an independent authority, as opposed to one with public oversight.

8. Cooperation and Coordination

Section 24 calls for cooperation and coordination among government authorities and states that, among other things, authorities should take part in associations, working groups, and joint fora that contribute to adopt joint positions. We note that certain restrictions are in place that would prevent the authorities in some jurisdictions from fully participating in the activities of some organizations. For example, the ICDPPC will only accept an authority as a full member if it meets certain criteria. We think it would be advisable to allow the full participation of all authorities whose competency includes some form of data privacy enforcement.

[13] *See* http://curia.europa.eu/jurisp/cgi-bin/form.pl?lang=EN&Submit=Rechercher$docrequire=alldocs&numaff=C-518/07.

9. Liability

The first paragraph of Section 25 states that the responsible party is liable for the pecuniary and/or non-pecuniary damages caused to the data subjects as a result of processing in violation of the applicable laws, "except if the responsible person can demonstrate that the damage can not be attributed to him." It appears that this would place the burden of proof on the "responsible party" to demonstrate that it was not responsible. This should be clarified.

Also, it is unclear what situations are envisioned where the responsible party might be able to demonstrate that the damage can not be attributed to him. This language could refer to situations where the service provider's actions resulted in the damage. It is not clear whether this Section is suggesting that the responsible person can be relieved of liability if the failure was on the part of the service provider.

Paragraph 2 sets forth that States will facilitate the access of data subjects to the judicial and administrative processes. It is not clear what kind of facilitation is contemplated and whether there is a requirement beyond consumer education about available processes.

Paragraph 3 of this Section then states:

> *[t]he aforementioned liability should exist without prejudice to the penal, civil or administrative penalties provided for, where appropriate, in case of violation of the provisions of domestic laws on the protection of privacy with regard to the processing of personal data.*

It is unclear whether this paragraph is suggesting that the liability set forth in Section 25 would exist regardless of the penalties set forth in a country's national law. The intent of this paragraph should be clarified.

* * *

We 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 John Kropf, Deputy Chief Privacy Officer, DHS, john.kropf@dhs.gov, 703-235-0780. Thank you.