Comments on the Joint Proposal **(version 3)** for a Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data

May 14, 2009

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") in their capacities as observers to the International Conference of Data Protection and Privacy Commissioners (ICDPPC).[1]

We appreciate the opportunity to submit these comments on **version 3** of the Draft of International Standards on the Protection of Privacy with regard to the processing of Personal Data (the "Standard"). This project provides an additional forum to engage in the important international dialogue on the different approaches to privacy and the areas of common ground. The Agencia Española de Protección de Datos ("AEPD") has provided us with the opportunity to provide our input on this initiative and we thank them for allowing us to offer our perspective.

In connection with this project, we have had the opportunity to participate as observers in the experts meeting that took place in Barcelona in January 2009 and we expect to participate in the June 2009 meeting in Bilbao. The points we raise below are based on our participation in the January meeting, as well as version 3 of the draft text of the Standard and the explanatory memorandum previously circulated.[2] The points below raise questions and concerns about the Standard, including whether the timeline outlined for the Standard is feasible considering the ambitious reach of the project and the array of issues requiring thorough analysis.

1. Scope.

As a preliminary matter, data privacy is a highly complex and technical subject in which there remain significant unresolved political and policy debates. We point out that the United Nation's International Law Commission has noted that data protection is an area "in which State practice is not yet extensive or fully developed."[3] Accordingly, we question whether the topic is sufficiently advanced in terms of State practice to permit a useful global standard.

---

[1] These comments do not represent an official position of the United States government or any of its agencies. Rather, they represent the views of FTC staff and the DHS Privacy Office.

[2] We understand that a new version of the explanatory memorandum will be circulated shortly, but we have not seen it at the time of these Comments.

[3] 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.

We also note that international conventions typically cover a narrow issue with broad consensus. This proposal 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. We also note that the project's magnitude poses challenges to moving it forward. As currently drafted, the Standard would apply to all "the processing of personal data wholly or partly by automatic means, carried out by the public or the private sectors." This broad application, which includes the "public sector," requires clarification.

Queries: ***Which areas of government are intended to be covered by the term "public sector"? What different policy issues are raised by addressing a binding instrument to private entities, public agencies, and agencies with police, public order, and/or national security powers?***

Proceeding from the answer to the first question raised immediately above, we recommend that those entities affected by this initiative be included in this dialogue. Also, to the extent that the Standard contemplates application to national security, regulatory, law enforcement, and public safety functions, we note that at this juncture, this initiative has excluded participation by the authorities directly responsible for those areas, both in the United States and in the countries that are represented in the ICDPPC. We recommend including representatives responsible for these areas in this project. Finally, we note that there is not a uniform approach to domestic privacy protections as to national security and public safety functions, even within the Member States of the European Union.[4]

2. Next steps. While this document is characterized as containing "International Standards," it is unclear whether it is intended to be a first step leading to a follow-up effort.

The ICDPPC adopted a declaration in 2005 appealing "to the United Nations to prepare a legal binding instrument which clearly sets out in detail the rights to data protection and privacy as enforceable human rights," and "to every Government in the world to promote the adoption of legal instruments of data protection and privacy according to the basic principles of data protection and also to extend it to their mutual relations."[5] This declaration was followed in

[4] 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.

[5] See Montreux Declaration on The Protection of Personal Data and Privacy in a Globalised World: a universal right respecting diversities (September 2005), available as a pdf file at http://www.edoeb.admin.ch/dokumentation/00444/01023/01025/index.html?lang=en.

October 2008 by a resolution describing a variety of "promising" efforts undertaken in a number of different fora.[6]

Query: ***Does this project aim to be the stepping stone for a United Nations convention?***

In order to obtain meaningful input from the appropriate stakeholders, as discussed throughout these comments, it is important for there to be transparency in connection with this project and the intended next steps.

3. Applicable Law and Jurisdiction. Section 25 (1) of the draft Standard states that the law that will apply to the processing of personal data will be the law where the "responsible person" has an establishment. Section 25(2), however, states that if the "responsible party" does not have an establishment in a particular territory but addresses its activity to that territory, the applicable law in such a case will be the law of the territory where the activity is directed. Assume that a company based in country X markets its products to individuals in country X, and collects and processes the personal information of these individuals. Section 25(1) suggests that the applicable law of country X would apply. Assume that this same company also targets individuals in country Y, and collects and processes the personal information of individuals in country Y. Section 25(2) suggests that the law that would apply is the law of country Y.

Query: ***Is it correct to say that with regard to the scenario described above, if Section 25 of the Standard were applied, the conclusion would be that with regard to the company's transactions with individuals with country Y, it would not be governed by the law of country X -- -- the law in which the company is located? The law of country X, however, may require the company to comply with the laws of country X regardless of the location of the customer -- -- the Standard does not appear to address how conflicts of law questions might be resolved.***

Conflicts of law rules are not consistent across jurisdictions, and as noted recently by European Commission (EC) staff in a report on cross-border e-commerce in the EU, they are implemented differently by Member States.[7] The EC staff point out that the compliance costs of operating in several Member States is a barrier to cross-border selling, and that it is crucial to address these market barriers. We

---

[6] See Resolution on the urgent need for protecting privacy in a borderless world, and for reaching a Joint Proposal for setting International Standards on Privacy and Personal Data Protection (the "Resolution"), available at http://www.privacyconference2008.org/adopted_resolutions/STRASBOURG2008/resolution_international_standards_en.pdf.

[7] Commission Staff Working Document, *Report on cross-border e-commerce in the EU*, March 5, 2009, SEC(2009) 283 final, at p. 15, *available at http://ec.europa.eu/consumers/strategy/docs/com_staff_wp2009_en.pdf*.

question whether the provisions of the Standard will resolve the conflicts of laws issues that will inevitably remain due to national laws.

The difficulties relating to applicable law, conflicts of law and jurisdiction are ones that are continuously being discussed in various fora, as the issues are complex and workable resolutions are difficult to achieve. In connection with the Hague Convention on Jurisdiction and Foreign Judgments in Civil and Commercial Matters (the "Judgments Project"), it was noted that the growth of the Internet has created additional challenges in developing standards with regard to applicable law, jurisdiction and conflicts of law questions.[8]

The challenges relating to applicable law with regard to online commerce were discussed in some detail in a 1999 FTC report.[9] In this report, the FTC noted that some favor a "country of destination" system, where consumers could rely on the law in their own country to govern their transactions, while others supported a "country of origin" or "prescribed-by-seller" rule, which would subject companies to the laws of their own country (or as prescribed by contract). The report suggests some of the difficult questions that arise in this area.

It is unclear whether the Standard seeks to address conflicts that might arise between data protection and other laws, for example, those relating to consumer protection and contracts. Finally, note that an additional layer of complication arises from the interaction of choice of court and choice of law issues, and a layer beyond that from the interaction of public and private rights of action.

Query: ***What analysis has been done in connection with this project on the options for applicable law, and the likely market impacts of those options?***

4. Self-regulation. Section 21(g) provides that States should encourage "the adoption of codes of self-regulation the observance of which is binding, that include elements that allow to measure its efficiency as far as compliance and level of protection of personal data are concerned, and that set out effective measures in case of non compliance." It is unclear what is being contemplated by "effective measures in case of non compliance."

Query: ***Does the Standard contemplate government backstop enforcement in the event of noncompliance with self-regulatory requirements?***

---

[8] *See* Avril D. Haines for the Hague Conference Permanent Bureau, *The Impact of the Internet on the Judgments Project: Thoughts for the Future, Preliminary Document No 17 of February 2002* at 10, available as a link at http://www.cptech.org/ecom/jurisdiction/hague.html.

[9] Consumer Protection in the Global Electronic Marketplace, available at http://www.ftc.gov/bcp/icpw/lookingahead/electronicmkpl.pdf.

Also, we note that the ICDPPC Resolution called for the drafters "to examine the role to be played by self-regulation."[10] This examination should be conducted before determining what role self-regulation should play in an international standard. As part of this study, it would be useful to consult with organizations such as APEC, whose members are currently developing a mechanism for cross border data transfers that contains self-regulatory elements.

We also note that the prior version of the Standard contained references to self-regulation in connection with alternative dispute resolution, but those references have been removed in this version.

Query: ***What is the rationale for removing references to alternative dispute resolution?***

Also, private-sector industry initiatives could be useful in developing cross-border mechanisms to protect data transfers, and it would be useful to consult with the private sector as part of the study examining self-regulatory mechanisms in the data protection area.

5. Cultural Differences. A jurisdiction's approach to privacy, and corresponding legislation, may be unique to its country's culture and values. In fact, the Commissioners ''[r]ecognise that countries have adopted different approaches to protecting personal information and enhancing privacy rights.''[11] 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 dimension in many jurisdictions -- that affect how privacy is approached.[12] We question how it is possible for an international standard to work through all these issues and develop

[10] See Resolution, at paragraph 3.

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

[12] 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).

sufficient common ground in a way that will add to the already existing guidelines (for example, the 1980 OECD Privacy Guidelines, and the APEC Privacy Framework).

a. International Transfers

One area in particular that requires further analysis and clarification is the Standard's requirements with regard to international transfers. Version 3 of the standard provides that "international transfers of personal data may be carried out when the State or organization recipient of such data afford a substantially similar level of protection to that one providing in this Document." We note that the previous version required only a similar level.

Query: ***A "substantially similar" level of protection appears more restrictive than a "similar" level -- -- what is the rationale for modifying the Standard?***

We raise the concern that a "substantially similar" analysis may offer even less flexibility than an "adequacy" analysis. The ICDPPC Resolution to pursue this work actually states that one of the considerations in developing a standard is formulating "the essential guarantees for better and flexible international transfers of data."[13] (Emphasis added.) We also point out that the Resolution calls for a standard to "aim to achieve the maximum degree of international acceptance ensuring a high level of protection."[14]

Queries: ***Considering that the EU experience has resulted in an adequacy determination for only a few countries outside the EU after more than a decade, how will a "substantially similar" standard, which appears more restrictive offer greater flexibility in international transfers of data? Similarly, is such a standard likely to achieve the maximum degree of international acceptance?***

We also note that the Standard states that supervisory authorities may assess the "concurrence in the recipient of a substantially similar level of protection to that one provided in the Document."

Query: ***Does the Standard contemplate that all international transfers will need prior approval of the supervisory authority, so that a determination can be made as to level of protection offered by the recipient?***

It is important to clarify the Standard's intent with regard to international transfers and elaborate what mechanisms would be necessary to effectuate transfers. It is also important to consider the policy implications of requiring that supervisory authorities play a certain defined role in every country.

[13] See Resolution, at paragraph 3.

[14] See Resolution, at paragraph 3.

b. Exclusions

The Standard states that countries may exclude the application of the "whole or a part of the provisions of this Document, 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." The circumstances under which exceptions will be permitted will not be consistent across jurisdictions due to differing legal frameworks and cultural differences. For example, jurisdictions use different criteria to determine whether there is a public health emergency that would warrant actions counter to the provisions in the Standard. With regard to national security, jurisdictions may make different determinations as to whether there is a credible risk to national security.

Query: ***Will the inconsistent application of the "exceptions" to the Standard negate the underlying goal of the Standard to create a uniform data protection framework?***

We also note that the previous version of the Standard provided that States may also exclude the application of the Standard in whole or in part in the interests of "the economic well being of the country" and "for the prevention of disorder or crime." These exclusions, however, have been removed in this current draft. The economic well being of a State and the prevention of disorder or crime are important state interests -- -- it is necessary to allow States the discretion in the application of the provisions of the Standard to protect these interests.

Query: ***What was the rationale for removing these exclusions?***

c. Private and Family Life Processing

The Standard states that its provisions would 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, where the processing does not infringe the rights and freedoms of others." As stated previously, due to cultural differences, as well as different legal systems, what constitutes a "right" or a "freedom," will not be uniform across jurisdictions. Accordingly, the exception to the otherwise permissibility of processing relating to private and family life will not be consistently applied across jurisdictions.

Query: ***In an ever growing globalized world, where family members and social networks expand across jurisdictions, how could natural persons become educated about the different standards relating to what is permissible in the processing of personal data relating to private and family life?***

We also note that this language in the Standard appears to go beyond that found in any international instrument. It is also more restrictive than the text of the EU

Data Protection Directive, which 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."[15]

Queries: ***What is the rationale for this expansion of the reach of data protection laws? How will these restrictive requirements with regard to personal processing, which appear to be the most restrictive in any data protection instrument currently in effect or contemplated, "achieve the maximum degree of international acceptance ensuring a high level of protection?"***[16]

Moreover, inconsistent standards across jurisdictions with regard to personal and household processing will create the same challenges that we are seeking solutions for in the commercial context -- -- the imposition of regulatory borders on activity relating purely to personal or household functions.

6. Cooperation and Coordination.

The Standard 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.

Query: ***Wouldn't it be advisable to encourage organizations to allow the full participation of all authorities whose competency includes some form of data protection enforcement?***

7. Broader Participation. Generally, the development of an international standard, regardless of the subject matter, requires broad input. In this case, the privacy-related draft standard is being launched by the membership of the ICDPPC. This organization is limited only to jurisdictions with a certain type of privacy framework (indeed the United States is not a member). In fact, the Resolution calls for the draft Standard to be submitted to the closed session.[17] Many countries, including many populous ones, are not represented in this process. The ICDPPC represents in round numbers only about a tenth of the worlds' population.

---

[15] 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; Article 3.

[16] See Resolution, at paragraph 3.

[17] See Resolution, at paragraph 3.

Query: ***What is the rationale for evaluating the Standard within the closed session where only representatives of accredited authorities are able to participate?***

If an international standard is to be meaningful, it would appear to require input and broad participation by the governments of nations around the world, regardless of their approach to privacy. Discussing this initiative in an open setting would provide the opportunity for a wider range of participants to attempt to reach consensus in an area whose importance merits participation by all stakeholders. In addition to individual governments, a proposal for an international standard relating to privacy would benefit from the input of relevant stakeholders, including international organizations that devote significant resources to international privacy issues, e.g., the OECD's Working Party on Information Security and Privacy, and the Data Privacy Subgroup of APEC's Electronic Commerce Steering Group. In addition, industry groups could offer the perspective of business, which would be valuable input to the discussion of a proposed standard. In addition, consumer organizations, as well as the public, would add another important perspective to this dialogue which is essential in examining the issues raised in a draft privacy standard. We encourage reaching out to these stakeholders to participate in the discussions relating to this project.

Query*: Does the ICDPPC intend to consult with the fora mentioned as well as nations not represented by these groups in order to achieve broad-based input?*

8. New technologies. In an era where technology changes and develops at rapid speed, it may not be advisable to develop an international convention that would be difficult to modify. Jurisdictions contemplating regulatory or legislative solutions to new and emerging technologies will not want to be bound by an international convention that may create obligations that are unrealistic in the face of a changing technological landscape. For example, the use of RFID technology, sensor-based networks, and identity management systems all would implicate the elements raised in this draft standard. In order to respond appropriately to the landscape in its own jurisdiction, nations need a certain level of flexibility when they contemplate regulatory or legislative responses relating to new and emerging technologies.[18]

Query: ***How can such a Standard adapt to changes in policy and technology?***

[18] We note by way of comparison that the overall EU structure provides for a mechanism to change directives, and that the European Commission is holding a conference in May to address such issues as the following: "How should personal data be protected in the wake of modern technologies and new policies? How well are current rules on international transfers of personal data working in a time of 'cloud computing'?" See conference announcement *available at* http://ec.europa.eu/justice_home/fsj/privacy/news/docs/pr_03_03_09_en.pdf.

Considering rapidly evolving technologies, it would be important for such an instrument to have some meaningful way of making any necessary adjustments.

9. Data Breaches. Section 19(2) of the Standard requires the notification to data subjects of data breaches "that could significantly affect their pecuniary or non-pecuniary rights, as well as its harmful effects and the measures taken for its resolution."

Legal requirements in this area are only beginning to develop, 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. Currently there are legislative initiatives in both the European Union and the United States (on a Federal level) recommending data breach notification relate to specific categories of information. For example, the European Parliament adopted text on May 6, 2009 that amends the ePrivacy Directive,[19] requiring notification to individuals in the event of a breach relating to publicly available electronic communications services.[20] In the United States, the Federal Trade Commission recently published a proposed rule that would require entities to notify consumers when the security of their electronic health information is breached.[21] Different categories of information may warrant different criteria in determining whether breach notification is necessary.

As stated earlier, setting the specified criteria for when breach notification is required may be difficult when legislatures are still evaluating this issue, often resulting in different standards. For example, in the United States, more than 40 states now have breach notification laws, many of which differ from one another.[22] Also, the European Parliament has provided for national differences

---

[19] Directive 2002/58/EC Of The European Parliament And Of The Council Of 12 July 2002 Concerning The Processing Of Personal Data And The Protection Of Privacy In The Electronic Communications Sector (Directive On Privacy And Electronic Communications).

[20] *See* Position of the European Parliament adopted at second reading on 6 May 2009 with a view to the adoption of Directive 2009/.../EC of the European Parliament and of the Council amending Directive 2002/22/EC on universal service and users' rights relating to electronic communications networks, Directive 2002/58/EC concerning the processing of personal data and the protection of privacy in the electronic communications sector and Regulation (EC) No 2006/2004 on cooperation between national authorities responsible for the enforcement of consumer protection laws, *available at* http://www.europarl.europa.eu/sides/getDoc.do?pubRef=-//EP//TEXT+TA+P6-TA-2009-0360+0+DOC+XML+V0//EN&language=EN#BKMD-15.

[21] *See* http://www2.ftc.gov/opa/2009/04/healthbreach.shtm for the press release announcing the proposed rule and a link to the text of the proposed rule. Procedurally, publication of the proposed rule is the first step in the process of approving a final legally enforceable rule. Currently, the FTC is accepting comments on the proposed rule – the comment period closes on June 1, 2009.

[22] *See* http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm.

in this area -- -- in the amendments to the ePrivacy Directive relating to breach notification, the text reads as follows:

> *[s]ubject to any technical implementing measures adopted under paragraph 5, the competent national authorities may adopt guidelines and, where necessary, issue instructions concerning the circumstances in which notification by providers of personal data breaches is required, the format of such notification and the manner in which the notification is to be made.* [23]

Accordingly, at this time it would seem difficult to set forth specific criteria that triggers the data breach notification requirement. In addition, setting forth specified criteria may not allow for special circumstances. For example, with regard to the requirement in the Standard to inform data subjects of the measures taken in connection with a 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.

10. Timeline. Our understanding is that the International Conference of Data Protection and Privacy Commissioners will next meet in Madrid in November 2009. We understand that the goal is for the text of this Draft Privacy Standard to be finalized by this event. This date is six months away. Generally, an international standard is debated over the course of several years to allow for rigorous dialogue and sufficient input from all interested stakeholders. We are concerned about the very short timetable for this project and question whether an international standard can be developed in this short amount of time.

Query: ***What are the costs and benefits of proceeding according to this accelerated timeline?***

* * *

We appreciate the opportunity to provide these Comments, and look forward to hearing responses to the queries we have raised. We would also 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.

[23] *See supra* note 20.