THE INTERNATIONAL LEGAL FRAMEWORK FOR DATA PROTECTION AND ITS TRANSPOSITION TO DEVELOPING AND TRANSITIONAL COUNTRIES

December 28, 2004

One of the pre-conditions for development of the Information Society is for users to have confidence or "trust" in the reliability, security, and integrity of electronic communications systems and computerized information processing systems. Individuals will not readily use networks or systems they do not trust. In the absence of trust, individuals will refuse to disclose personal information, or they will give false information. One crucial component of the trust framework is privacy protection – the provision of assurances by means of law, technology design, and industry practice that personal information will be collected, exchanged and used fairly.

Information privacy or data protection in this context is not about keeping personal information secret; rather, it is about creating a trusted framework for collection, exchange and use of personal data in commercial and governmental contexts. Data protection laws permit, and even facilitate, the commercial and governmental use of personal data while providing to individuals (1) control over what to disclose; (2) awareness of how their personal data will be used; (3) rights to insist that data are accurate and up-to-date; and (4) protection when personal information is used to make decisions about a person.

As the global Information Age continues to evolve, international understanding of the policy options for data protection also evolves, guided by an understanding of the practical consequences and effectiveness of such laws.

Twenty-four years ago, the Organization for Economic Cooperation and Development (OECD) concluded that privacy protection was an important human right but that inconsistent national privacy laws might slow the realization of the economic and social benefits of the Information Age. In 1980, an international team of experts convened by the OECD developed a set of Privacy Guidelines, consisting of definitions, eight Privacy Principles, and enforcement approaches.[1] The OECD guidelines were intended to offer harmonized protection of individual privacy rights while being flexible enough to apply across a variety of

[1] http://www.oecd.org/document/20/0,2340,en_2649_34255_15589524_1_1_1_1,00.html.

social, legal, and economic circumstances. The 1980 OECD Guidelines have had enormous influence, finding their way into a variety of legislative and self-regulatory adaptations.

In 1995, the European Union adopted its Data Protection Directive (95/46/EC), establishing a detailed privacy regulatory structure for adoption into national law by EU member states.[2]

More recently, the International Chamber of Commerce has explored the impact of regulation upon the growth of information age business and concluded that the 1980 guidelines remain sufficient to protect individual privacy rights. In its Toolkit for Policy Makers, http://www.iccwbo.org/home/e_business/word_documents/TOOLKIT-rev.pdf, the ICC offers common sense advice, urging that privacy regimes be judged in terms of their practical effectiveness.

In November 2004, the twenty-one economies that make up the Asia Pacific Economic Cooperation forum endorsed an APEC Privacy Framework, a streamlined set of international norms or guidelines, based on the core fundamentals of the 1980 OECD Guidelines.[3] See Appendix A.

-- The OECD Privacy Guidelines:

The OECD Guidelines were intended as broad, minimal and internationally-applicable principles to guide a harmonized approach to privacy regulation around the world. In matters of definition and scope, the OECD Guidelines --

- Defined personal data as information relating to an identified or identifiable individual (a natural person).
- Recognized the need for greater protections of certain categories of "sensitive" personal information, such as health data, for example.
- Created the concept of the data "controller," which is defined as the party with legal competence to decide the contents and use of personal data. The data controller is the party ultimately responsible for particular data. (Since data can be copied, there may be more than one controller for a specific item of information.)
- Were applicable to both governmental and commercial use of data.
- Allowed exceptions for national sovereignty, security, and public policy but urged that the exceptions be narrow.

---

[2] http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

[3] Available at http://www.apecsec.org.sg/apec/news___media/media_releases/201104_apecminsendorseprivacyfrmwk.html.

- Recognized privacy as an important but not absolute right, recommending that strong privacy protections should be balanced with the economic and social value of participation in an international information economy.

- Encouraged self-regulation, including the development of industry codes

- Sought to minimize restrictions on transborder data flows.

The OECD Guidelines set out eight basic Privacy Principles:

1. **Collection Limitation.** There should be limits on data collection, and data should be obtained by fair and lawful means and, where appropriate, with the knowledge or consent of the data subject.
2. **Data Quality.** Data should be relevant to the purposes for which it is collected and should be accurate, complete, and up to date.
3. **Purpose Specification and Notice.** The purpose for which data are collected should be provided to the data subject no later than at the time of collection; the subsequent use of dated should be limited to those and other "not incompatible" purposes.
4. **Use Limitation**. Data should not be disclosed or used except for purposes specified in the notice unless the data subject consents or the law requires disclosure.
5. **Security**. Requires "reasonable" safeguards for personal data.
6. **Openness**. Requires openness about practices and policies regarding personal data; it should be made easy to identify a data controller, how to reach it, the kinds of data it collects and the main purposes of that collection.
7. **Access**. Requires "reasonable" access by a person to data collected, or information about that data, and right to challenge, including requiring erasure of inaccurate data.
8. **Accountability**. The data "controller" should be accountable for complying with the protections and should be liable for harm.

-- The 1995 EU Data Protection Directive

The 1995 EU Data Protection Directive (95/46/EC) requires EU member states to enact national data protection laws complying with the Directive's standards.[4] The Directive adopts the OECD's definitions of personal and sensitive data, the eight Privacy Principles of

[4] In 2002, the EU adopted a second privacy directive, specifically addressing privacy in electronic communications services. Among other issues, the 2002 Directive on Privacy and Electronic Communications addresses unsolicited email and the use of personal information by communications companies. Both the 1995 Directive and the 2002 Directive are available at http://europa.eu.int/comm/internal_market/privacy/law_en.htm.

the OECD Guidelines and the concept of data controller. The Directive, however, makes several important changes or additions to the OECD Guidelines:

- It creates a "legitimacy" principle, found in Article 7, prohibiting any data processing operation that does not have a legitimate purpose (or unambiguous consent of the individual) within defined criteria. In doing so, the Directive requires a regulatory scheme in which national authorities retain the power to challenge or review any processing operation.

- It interprets the Openness Principle to require national registration of databases and data controllers.

- It promotes the free flow of information only between and among EU member states. Cross border transfer to other countries is prohibited unless the other country is found to provide an "adequate" level of protection, subject to certain exceptions.

- The Directive specifically requires member states to encourage use of codes of conduct, providing a means to limit discretionary exercise of authority and a flexible means to update national interpretation.

-- The APEC Framework

In November 2004, the twenty-one member economies of the Asia-Pacific Economic Cooperation forum endorsed a Privacy Framework.[5] Several aspects of the APEC Framework are worth noting here:

- Recognizes "reasonable expectations" of privacy but gives greater emphasis to the benefits of participation in a global information economy.

- Specifically endorses "proportionality" in national regulation. Regulation and remedy should be proportional to the likelihood and significance of harm to an individual.

- Focuses on what it calls "core fundamentals" of the OECD Guidelines and on the use of the Internet itself to provide notice, consent, and control.

Criticized by some as too weak, the Framework is consistent with the OECD Guidelines and does emphasize the importance of privacy regimes in a region where, with some notable exceptions, countries have not yet adopted privacy protection laws. The Framework:

[5] The full Framework document is available at http://www.apecsec.org.sg/apec/news___media/media_releases/201104_apecminsendorseprivacyfrmwk.html.

- Adopts the OECD and EU definition of personal information.
- Adopts the concept of the "controller" as the accountable party and insulates those who are "instructed by" another to collect, process, use or transfer data.
- Endorses the Collection Limitation, Data Quality, and Security principles.
- Emphasizes the usefulness of providing individuals with mechanisms of choice (or opt out).
- Recognizes the importance of access and correction but adds two exceptions: Access need not be provided if "the burden or expense of doing so would be unreasonable or disproportionate to the risks" or disclosure to the individual would compromise security or the confidentiality of commercial information.
- Limits application of the Framework in the case of publicly available data.
- Introduces the concept of proportionality in privacy regulation: Specific obligations and remedial measures should be proportionate to the likelihood and severity of potential harm.
- Takes a practical, forward-looking approach to the Notice Principle, encouraging the use of web sites as a means to provide requisite information before or at the time of data collection.
- Recognizes the importance of "legitimate expectations" of privacy.
- Encourages a combination of legislative, administrative, and industry self regulatory measures as well as educational efforts by the member economies.
- Appears to be aimed primarily at commercial use of personal data.

Issues to Consider in Drafting national Laws

1. Consider first the national capabilities for implementation and the practical impact of the law's requirements.

The first step in drafting any new law is to assess the current legal framework, identify gaps in existing laws, and evaluate the institutional capacity of the nation to implement and enforce a new legal scheme. It is especially important for developing and transitional countries to approach Western or developed country models with caution. A law that establishes an administrative and normative structure that will be too complicated to implement could impede the development of the Information Society.

Merely transferring EU law into a still-developing legal culture does not guarantee either an equivalent level of practical protection nor the flow of information necessary for the development of the Information Society. The EU Data Protection Directive, if read and enforced literally, is quite broad. EU member states have means to take advantage of technology and avoid disproportionate impact upon business and upon participation in a global Information Age. These include varying degrees of enforcement, a tradition of industry self-regulation, and reference to industry codes. For example, EU concepts are based on the existence of a highly developed private sector that engages in self-regulation and co-regulation with the governmental bodies, thereby avoiding unnecessary burdens on commerce. Strict transposition of EU concepts into an environment lacking private sector institutions may impede economic activity

2. Consider the role of the government vis-à-vis the commercial sector

An related question concerns the role of the government: To what extent will data processors be required to report their practices to a central governmental authority, versus to what extent will data holders have obligations directly to data subjects to inform them about the data processing practices of such holders? The EU Directive takes a centralized approach. For a transitional nation, this may not be desirable – it may limit flows of information necessary to development of the Information Society while also putting too much information and power in the hands of the government. Policymakers need to consider what are the risks and benefits of a government-controlled Register of data files. Instead, for example, should data holders be required to make available, online or at their principal office for inspection, lists of the categories of data that they hold?

3. In order to avoid unnecessary burdens on economic activity, permit flexible implementation

Experience with the data protection authorities of EU member states suggests that regulatory mandates can be exercised in very different ways and the level of burden to industry (in proportion to the resultant protections of individual rights) can be quite different. In order to avoid unnecessary bottlenecks and potential barriers to the growth data processing, two strategies can be considered:

- **Explicitly recognize the importance of industry codes and self regulation.** EU member states have a tradition of industry-government dialogue and the use of industry codes of conduct. The EU Directive explicitly encourages the use of such "self-regulatory" measures, thereby making the impact of the directive less burdensome. These codes allow regulation to be flexible, in order to keep pace with technological developments and with evolving industry practices. Codes can help avoid unnecessary regulatory barriers and can limit discretionary exercise of regulatory authority. (Self-regulation, of course, can never override express legislative requirements.) If industry sectors are still in developmental stages within the country, a new data protection authority may wish to make reference to codes of conduct developed by industry groups in the EU and otherwise to seek technical assistance from industry groups in the EU.

- **Explicitly recognize the principle of "proportionality" of regulation.** Broadly-written powers to regulate can be a barrier to economic growth, particularly in emerging market economies where trust between industry and government is still developing. An explicit commitment to exercise state regulatory power only as necessary, proportional to the likelihood of harm to individuals and the nature of the harm may be desirable.

For further information, contact Jim Dempsey, GIPI Policy Director, jdempsey@cdt.org