GLOBAL INTERNET POLICY INITIATIVE

Privacy and E-Government: Privacy Impact Assessments and Privacy Commissioners – Two Mechanisms for Protecting Privacy to Promote Citizen Trust Online

May 1, 2003

Privacy is widely recognized as a human right. Individuals should be confident that information about themselves will be handled fairly. This includes personally-identifiable information in the hands of government agencies. In providing services to the public and carrying out various functions, governments collect and use a wide range of personal information about their citizens (i.e., health records, tax returns, law enforcement records, drivers license data, etc.). With the shift towards electronic data management and the growth of the information society, governmental gathering, storing and processing of data have grown dramatically. The introduction of e-government and the electronic delivery of services have further expanded government collection of personally-identifiable data. A government's practices in collecting, retaining, and managing personal data about its citizens pose a wide range of privacy concerns.

Trust is crucial to the success of any online program, whether in the field of e-commerce or in the field of e-government. Privacy and security are in turn key elements of online trust. Individuals will not use services that do not handle personal data responsibly. Therefore, countries seeking to facilitate the efficient online provision of governmental services must protect the privacy of the information they collect. Two mechanisms that countries are adopting to address this need are the privacy impact assessment ("PIA") and the privacy commissioner.

I. What Privacy Principles Apply to E-Government?

Many countries have adopted national privacy or data protection laws.[1] Such laws may apply to data about individuals collected by the government, to personal data in the hands of private sector businesses, or to both. For our purposes here, we focus on the treatment of information in government databases, but the privacy principles are actually the same for both commercial and governmental data.

"Privacy" is not just a matter of what is kept secret. In the context of e-commerce and e-government, the right to privacy is really the right to control the use of personal information that is disclosed to others. Throughout the world, the privacy of information about individuals is guided by the principles of "fair information practices." These principles, which were

[1] For an international survey of privacy law, including country-by-country reports, see *Privacy and Human Rights 2002*, EPIC and Privacy International ("*Privacy and Human Rights*") http://www.privacyinternational.org/survey/phr2002/

authoritatively detailed by the Organization for Economic Co-operation and Development (OECD),[2] represent basic guidelines for responsible information practices that respect the interests of individuals. They form the foundation of many national and local privacy laws, international agreements on data protection, and various industry codes of best practices.[3] It is these principles that provide the framework for privacy impact assessments and the reference point for the work of privacy commissioners.

As expressed by the OECD and other international bodies, fair information practices include:

- **Collection limitation**: No more information should be collected than is necessary to complete the transaction, and any such data collected should be obtained by lawful and fair means and, where appropriate, with the knowledge or consent of the data subject.
- **Data quality**: Personal data should be relevant to the purposes for which they are to be used, should be accurate and complete, and should be kept up-to-date.
- **Purpose specification**: When personal data are collected, the purpose for the collection should be specified and the subsequent use limited to the fulfillment of that purpose or such others as are not incompatible with the original purpose.
- **Use limitation**: Personal data should not be disclosed, made available or otherwise used for purposes other than those specified in accordance with the "purpose specification" except: (a) with the consent of the data subject; or (b) by the authority of law.
- **Security**: Personal data should be protected by reasonable security safeguards against loss or unauthorized access, destruction, use, modification or disclosure.
- **Openness**: In general, there should be no secret collections of data. As a matter of general policy, there should be openness about data practices and policies. Means should be readily available to individuals to establish the existence and nature of databases, the main purposes of their use, and the identity of the entity responsible for the database.
- **Individual participation**: An individual should have the right to obtain access to any data about him held by a data controller. This includes (a) confirmation of whether or not an entity has data relating to him; (b) to obtain copies of data relating to him within a

---

[2] OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, 1980, http://www.oecd.org/EN/document/0,,EN-document-0-nodirectorate-no-24-10255-0,00.html.

[3] The OECD principles were in turn based on the Code of Fair Information Practices developed in the 1970s by the U.S. Department of Health, Education and Welfare. *See* U.S. Dept. of Health, Education and Welfare, Secretary's Advisory Comm. on Automated Personal Data Systems, *Records, Computers, and the Rights of Citizens*, July 1973. Since then, the principles of fair information practice have been reflected not only in the OECD guidelines but also in the following major international instruments on data privacy:

- Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, Council of Europe Convention No. 108 (1981);
- UN Guidelines for the Regulation of Computerized Personal Data Files (1990);
- EU Directive on Data Protection (1995).

reasonable time; at a charge, if any, that is not excessive; in a reasonable manner; and in a form that is readily intelligible; (c) to be given reasons if a request made under subparagraphs (a) and (b) is denied, and to be able to challenge such denial; and, (d) to challenge data relating to him and, if the challenge is successful, to have the data erased, or corrected or completed.

- **Accountability**: Entities collecting data should be subject to enforcement measures that give effect to the principles stated above.

There are obvious exceptions to some of these principles in specific applications. For example, in the context of law enforcement investigations, it is not always possible to give notice to a suspect or to give him access to the information that the police are collecting. Nevertheless, these principles provide a framework for thinking through the privacy issues raised by any government collection of personal information.[4]

II. Privacy Impact Assessments

-- What is a Privacy Impact Assessment?

Although the precise definition may vary from jurisdiction to jurisdiction, a privacy impact assessment ("PIA") can be defined as "an assessment of any actual or potential effects that an activity or proposal may have on individual privacy and the ways in which any adverse effects may be mitigated."[5] Thus, PIAs are used to evaluate the privacy impact of computerization or data collection projects proposed by government entities, in the same way that environmental impact assessments are used to identify and evaluate the environmental impact of projects like dams or highways.

A privacy impact assessment provides a framework for identifying and addressing privacy issues. Specifically, the PIA is an evaluation that is conducted to assess how the adoption of new information policies, the procurement of new computer systems, or the initiation of new data collection programs will affect individual privacy. To the extent that the proposed action or program is found to pose a risk to privacy, the PIA recommends changes in the technology or policies in order to avoid or mitigate the adverse effects on privacy.

---

[4] "Personal (or personally-identifiable) information" is data that can be associated with an individual. Notably, a person's name need not be attached to the information for it to qualify as "personal information." For example, data categorized by a unique numeric identifier is considered personal information even where no name is attached to it, since the numeric identifier can be used to determine the name.

[5] Blair Stewart, *Privacy impact assessments*, Privacy Law and Policy Reporter (1996) http://www.austlii.edu.au/au/journals/PLPR/1996/39.html. Blair Stewart, Assistant Commissioner, Office of the Privacy Commissioner, New Zealand, is one of the main originators of the concept of the PIA.

The PIA measures whether proposed new technologies and policies will comply with any relevant national privacy legislation and also seeks to identify any broader privacy implications with reference to internationally-recognized privacy principles.[6]

-- What is the goal or purpose of a Privacy Impact Assessment?

PIAs evaluate the privacy issues (i.e., the fair information practices) related to personal data collection or usage in new or revised government activities and recommend protections to mitigate any negative impact on privacy. PIAs also can identify privacy concerns related to proposed law enforcement or security programs involving government surveillance, such as the monitoring of individuals' activities or communications.

The PIA process seeks to ensure that privacy issues are identified and addressed by policy makers at the initial stages of a new project or policy -- at the conceptual stage, the design approval stage, and the funding stage. The premise of the PIA is that considering and addressing privacy issues at the early stages of a project cycle will reduce the potential that the project will be found to have an adverse impact on privacy after it has been implemented, when it may be difficult to mitigate the impact. Thus, PIAs help avoid costly redesigns or cancellations of projects.

PIAs should be distinguished from compliance audits, which are designed primarily to ascertain whether a project as implemented meets the legal requirements of applicable privacy laws. PIAs should go beyond a strict legal audit by identifying optimum privacy options and recommending solutions to apparent deficiencies in data practices. A PIA provides decision makers with full knowledge and information regarding the privacy implications of the various policy options they consider during the course of their decision-making on a particular project or program that will involve data collection.

-- What types of projects warrant PIAs?

A PIA should be performed on any government proposal that involves the collection, use, or disclosure of personal information. For example, PIAs should be triggered by major purchases of IT system that will process personal information or by upgrades that will change the functionality of systems handling personally-identifiable data. Typical projects where PIAs should be undertaken include:

---

[6] For example, the Office of the Privacy Commissioner in New Zealand notes that both national and international privacy standards are relevant to PIA. The Privacy Commissioner adds –

> "depending upon the proposal being assessed there may be supplementary international or national guidelines. Occasionally these will be specified in national law, for example, the public register privacy principles in the New Zealand Privacy Act. In others, reference may be had to guidelines issued by such bodies as the Council of Europe, EU, ILO, OECD, UN and ISO." See http://www.privacy.org.nz/media/pia.html

- creation of public health databases;
- interlinking of existing databases or merging of public registries into a "super registry;"
- new law enforcement surveillance projects;
- proposals to adopt a national ID card, or to add new biometrics to existing ID systems;
- proposals to give law enforcement agencies new powers to access computer systems;
- any proposed law that would require private businesses to collect information on their customers;
- assignment of new personal identifiers by the government;
- creation of new databases or modifying the scope or use of databases that contain personal information;
- establishment of electronic toll systems on highways;
- expansion of data matching;
- the installation of closed circuit television in public places. [7]

Minor changes to existing government projects or programs would not generally trigger a PIA. Routine improvements or system maintenance, such as minor software upgrades or equipment replacement, do not require a PIA. Instead, a PIA should be performed in connection with significant project changes -- those that would increase the scope of collection, use or disclosure of personal information.

-- When should a PIA be performed?

Early identification of privacy risks is necessary to maximize the chances that a system can be redesigned to avoid or mitigate the negative privacy impact. Thus, to be meaningful, the PIA should be inform the decision making process associated with a particular project. Accordingly, it is most efficient to begin the PIA early in the project life cycle, at the conceptual stage of a project. However, since it may not be possible to conduct a full and detailed PIA until later stages in the system or program development, the PIA should be viewed as an evolutionary process that will become more refined as the project develops.

-- Who should conduct the PIA?

There should be independence in the PIA process. Some commentators therefore have suggested that, to insure credibility and objectivity, the PIA should be performed by an independent office or entity not linked to the project under review. In some instances the PIA could be performed by outside consultants, while in other instances it may suffice to assign staff members from another section of the organization.

---

[7] See *Privacy Impact Assessment Guidelines*, Freedom of Information and Privacy Office, t, Management Board Secretariat, Ontario, Canada (June 2001) http://www.gov.on.ca/MBS/english/fip/pia/index.html; and *Privacy Impact Assessment, PIA: Some Approaches, Issues and Examples*, presentation by Blair Stewart, Assistant Commissioner, Office of the Privacy Commissioner, New Zealand, available at http://www.pco.org.hk/misc/stewart/tsld001.htm

-- What are the outcomes of a PIA?

The PIA process identifies privacy risks and recommends design changes, procedures or policies that could be adopted to protect privacy. The risks and proposed remedies should then be considered by policy makers and used in making decisions regarding the proposed project.

The formal result of the PIA is a privacy impact report. Although the contents of each report will vary, there are several components that are frequently recommended.[8] These include:

- An overview that explains the subject organization's privacy policies and the assessment process that was used;
- A description of the proposed project, the types of personal information that will be collected or used and how it will be disseminated or retained;
- An explanation of who will have access to particular categories of personal data. (Employees should have access to the system only to the extent that is required for them to perform their duties. Procedures should be established to deter and detect browsing and unauthorized access.)
- A Privacy Analysis that identifies how the new project or practice will impact individual privacy. This analysis should highlight areas that may violate privacy laws, international norms or stated policies.
- A Risk Assessment that lists the privacy risks that have been identified and an analysis of how those risks may affect individuals and the success of the project.
- A discussion of appropriate technical, procedural or other responses or safeguards that can be adopted to enhance privacy.
- A discussion of how the project's privacy risks should be managed on a going forward basis.

This report and any associated recommendations should be made available to the public.[9] Public release of PIA findings can foster public trust in new systems. Given the potential wide readership of the report, the report should be drafted in language that is easily understood by non-technical readers. In addition to the public release of the findings, some commentators suggest that it also may be appropriate to hold a public consultation in some instances.

---

[8] See e.g., http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paipg-pefrld2_e.asp#6.3, which details Canadian PIA guidelines. For a more detailed discussion, see *Draft Guidance Notes on Codes of Practice under the Privacy Act: Privacy Impact Assessment Handbook*, Blair Stewart, Assistant Privacy Commissioner of New Zealand, available at http://www.privacy.org.nz/comply/pia.html. For another outline of the elements of the privacy assessment, see *Privacy Impact Assessments: an essential tool for data protection*, by David Flaherty (revised October 12, 2000) http://aspe.hhs.gov/datacncl/flaherty.htm.

[9] Canada, for example, requires PIAs to be posted on the Internet. New Zealand also requires the public release of these materials.

-- What countries are using PIAs?

PIAs are being used in Hong Kong, Canada, New Zealand, and Australia, and soon will be performed in the United States. Some of the approaches being pursued in different parts of the world are briefly described below.

Canada

The Canadian government was the first national government to make PIAs mandatory. Canada requires all federal departments and agencies to perform PIAs for all programs and services where privacy issues may be implicated.[10] Canada has adopted a PIA policy that provides a consistent framework for identifying and resolving privacy issues during the design or re-design of government programs and services. For example, Canada is developing a Government on Line project that will permit the delivery of government programs and services over the Internet. Recognizing the importance of fostering citizen trust and confidence in these planned online delivery systems, the Canadian Government is using the PIA process to design policies to protect the personal information of its citizens in connection with this initiative.[11] PIAs are made available on public websites..

New Zealand

New Zealand is another early leader in the use of privacy impact assessments. A discussion of the PIA principles followed in New Zealand is available at: http://www.privacy.org.nz/media/pia.html.

United States

In 2002, the U.S. Congress adopted legislation, the E-Government Act of 2002, which requires federal government agencies to conduct privacy impact assessments before developing or procuring information technology or initiating any new collections of personally-identifiable information.[12]

Under this new law, a privacy impact assessment must address what information is to be collected, why it is being collected, the intended uses of the information, with whom the

---

[10] General background information on Canada's policies with respect to PIAs is available at: http://www.tbs-sct.gc.ca/pubs_pol/ciopubs/pia-pefr/paip-pefr1_e.asp#Preface.

[11] *The Government of Canada – A World Leader in the Protection of Citizens' Personal Information*, issued by the Treasury Board of Canada Secretariat, April 24, 2002, available at http://www.tbs-sct.gc.ca/media/nr-cp/2002/0424_e.asp. Canada's Privacy Impact Assessment Policy is available at http://www.tbs-sct.gc.ca/pubpol_e.html.

[12] Links to the text and legislative history of the E-Government Act are available at: http://www.cdt.org/legislation/107th/e-gov/.

information will be shared, what notice would be provided to individuals and how the information will be secured. To the extent practicable, privacy impact assessments must be published. As of May 1, 2003, the Director of the White House's Office of Management and Budget (OMB) was developing guidelines for the assessments.

III, Privacy Commissioners

An essential aspect of any privacy protection regime is oversight and enforcement. A number of countries have created an office or agency to oversee privacy protection. Several countries including Germany, Canada and Australia also have officials or offices on a state or provincial level. The powers of these officials vary widely by country. Many have authority over both private sector and governmental databases.[13]

Most of the privacy commissioners are in member countries of the European Union. Under Article 28 of the European Union Data Protection Directive,[14] all EU members must have an independent privacy enforcement body. Under the Directive, these agencies are given considerable power: the commissioners have the power to conduct investigations and to access information relevant to their investigations; impose remedies such as ordering the destruction of information or banning its processing; engage in legal proceedings; hear complaints; and issue reports. Governments must consult the privacy commissioner when drawing up legislation relating to the processing of personal information. The commissioner is also generally responsible for public education.

Even if a country does not have a comprehensive privacy act, it can have a privacy commissioner. Even if the commissioner has no binding enforcement power, the ability to focus public attention on problem areas can be significant. Commissioners can do this by promoting codes of practice and encouraging government agencies (and industry associations) to adopt them. They can use press statements and reports to highlight problems.

A key to the success of a privacy enforcement agency is to provide it with adequate resources to conduct oversight and enforcement. Independence is also key. In countries where the agency is under the control of the political arm of the government or part of the Ministry of Justice, it may lack the power or will to criticize privacy invasive proposals of the government.

We summarize below some of the privacy commissioner systems that have been adopted.

---

[13] For a listing of the web sites of Privacy Commissioners, go to http://www.gilc.org/privacy/commissions.html. The Privacy Commissioner of Canada has also compiled links to Privacy Commissioners and privacy oversight officers around the world http://www.privcom.gc.ca/information/02_03_05_e.asp.

[14] 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, http://www.cdt.org/privacy/eudirective/EU_Directive_.html.

Australia

Australia's Office of the Federal Privacy Commissioner is tasked with creating a culture "in which privacy is respected, promoted and protected."[15] To achieve this goal, the duties of the office are to: provide policy advice; educate and inform the public about privacy issues, rights and responsibilities; and regulate compliance with Australia's privacy laws. Pursuant to legislation, the Commissioner's Office functions independently of direct political control by the executive branch.[16]

The Office of the Federal Privacy Commissioner has specific authority to:

- Investigate complaints from individuals about potential interference with their privacy;
- Conduct audits of the personal information handling practices of Commonwealth agencies;
- Inquire into acts or practices that may interfere with privacy;
- Foster public discussion, and undertake and coordinate research and education programs to promote the concept of privacy protection.

In Australia, privacy is regulated at both the federal and provincial level, so there are also privacy commissioners at the provincial level. In 1999, the Government of New South Wales, one of Australia's state governments, adopted a law establishing privacy principles for provincial government agencies. The act created the Office of the New South Wales Privacy Commissioner, an oversight entity that has authority to assist local agencies in complying with their state privacy obligations. The act empowers the state level commissioner: to advise government agencies, businesses and individuals on actions needed to protect the right to privacy; to research and report upon significant developments in policy, law and technology that impact privacy; and to make privacy recommendations to relevant authorities.

Canada

According to the Privacy Act and the Personal Information Protection and Electronic Documents Act, the Privacy Commissioner of Canada is responsible for ensuring that the federal government and companies in the private sector collect, use or disclose personal information in a manner that is responsible and transparent. These Acts governing personal information provide the Privacy Commissioner of Canada with the authority to ensure organizations and federal departments are held accountable for their information handling practices.[17] The Commissioner has authority to:

---

[15] See *The Operation of the Privacy Act Annual Report: 1 July 2001-June 2002*, Office of the Federal Privacy Commissioner at 18, online at http://www.privacy.gov.au. The Australian Privacy Act 1988 is at http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/

[16] *Privacy and Human Rights, supra*, note 1, at 105.

[17] http://www.privcom.gc.ca/faq/faq_01_e.asp#002.

- Publish information about personal information handing practices in the public and private sector;
- Conduct research into privacy issues;
- Promote awareness and understanding of privacy issues by the Canadian government and public; and
- Investigate complaints and conduct audits arising pursuant to federal privacy laws.

In terms of government databases, the Privacy Commissioner can consider complaints arising from the government's handling of personal information. These investigations seek to determine whether the privacy rights of individuals have been violated and whether individuals have been accorded the right of access to their personal information held by government agencies. Where privacy rights have been violated, the investigation process seeks to provide redress for individuals and to keep violations from recurring.[18] Ideally, complaints are resolved through negotiation, mediation and conciliation. If these voluntary efforts are not effective, however, the Commissioner has authority to conduct investigations, summon witnesses, administer oaths and compel the production of evidence.

The Privacy Commissioner is expected to function independently from other parts of the government in investigating complaints regarding government treatment of privacy issues. To ensure this independence, the Privacy Commissioner serves as an officer of the Parliament and reports directly to Canada's House of Commons and its Senate.[19]

Privacy commissioners also have been established at the provincial level to oversee the implementation of privacy-related legislation adopted by provincial governments.[20] According to the Electronic Privacy Information Center, nearly all of Canada's provinces have adopted legislation establishing data protection requirements for government agencies and creating oversight entities. However, the duties and powers vested within these provincial oversight bodies vary by region.[21]

Hong Kong

In 1996, Hong Kong adopted a Personal Data Ordinance that established fair information principles governing how certain public and private users handle "personal data" of citizens.[22] This ordinance also establishes a privacy oversight entity, the Office of the Privacy Commissioner for Personal Data, which is tasked with promoting and enforcing compliance with

---

[18] See http://www.privcom.gc.ca/au_e.asp.

[19] Id.

[20] See e.g., http://www.ipc.on.ca/scripts/index_.asp?action+31&N_ID=17&U_ID=0.

[21] *Privacy and Human Rights, supra*, note 1 at p. 143.

[22] Id. at p. 197.

the statutory requirements in the Ordinance.[23] The duties and powers vested in the Privacy Commissioner include:

- Promoting the awareness and understanding of the data privacy ordinance;
- Approving and issuing codes of practice that give practical guidance on compliance with the data privacy ordinance;
- Approving requests from data users on automated matching of personal data; and
- Inspecting personal data systems and making recommendations for compliance with the privacy ordinance.

In addition to these functions, the Privacy Commissioner has authority to investigate suspected breaches of the privacy law, and issue enforcement notices to data users as appropriate.

New Zealand

New Zealand's Office of the Privacy Commissioner ("OPC") is charged with several duties including:

- Promoting the goals of the nation's privacy legislation;
- Monitoring proposed legislation and government policies;
- Investigating and resolving privacy complaints;
- Approving and issuing codes of practice;
- Authorizing special exemptions from the information privacy principles;
- Monitoring government information matching programs; and
- Hearing complaints and acting as a conciliator in privacy complaints filed by citizens.

As in several other countries, the OPC is an independent government entity and, as such, is expected to function in a neutral manner when called upon to investigate citizen complaints against government ministries and departments, or to evaluate proposed legislation or regulations.[24]

Concluding Note

Countries seeking to promote e-government must protect the privacy of the information they collect. A country does not need to adopt comprehensive privacy legislation before conducting privacy impact assessments or appointing a privacy commissioner. Both PIAs and privacy commissioners may be good first steps in addressing privacy.

This memo was prepared by Paige Anderson, GIPI Staff Counsel, and Jim Dempsey, GIPI Policy Director. For more information, contact Jim Dempsey, jdempsey@cdt.org

---

[23] http://www.pco.org.hk/

[24] Annual Report of the Privacy Commissioner for the year ended 30 June 2002, at 11, available at http://www.privacy.org.nz.