

Privacy and E-Government

**A Report to the United Nations Department of Economic and Social Affairs
as background for the *World Public Sector Report: E-Government***

by

James X. Dempsey

Paige Anderson

Ari Schwartz

Center for Democracy and Technology

Washington, DC

(202) 637-9800

<http://www.cdt.org>

May 23, 2003

TABLE OF CONTENTS

I.	Introduction.....	1
A.	The Importance of Privacy as a Human Right and the Responsibility of the State in Protecting the Privacy of the E-Citizen	1
B.	Technology's Impact - Does Technology Redefine the Boundaries of Privacy?....	2
C.	Building Citizen Trust in New Government Systems	2
D.	Illustrative Case Studies Showing the Ways in Which Privacy Impacts E-Government Practitioners	3
1.	Japan – Juki Net.....	3
2.	Australia – PKI and Health Records.....	4
3.	US – Social Security Records Online	4
II.	Fair Information Practices - Defining Privacy	5
A.	The History of Privacy as a Human Right	5
B.	The COE/OECD/EU Principles	8
C.	Is Privacy Culturally Determined or International?	10
D.	Examples of Government Records Privacy Law Around the World	13
1.	Overview	13
2.	Selected Examples	14
a.	Republic of South Africa	14
b.	Hong Kong	15
c.	Canada.....	16
d.	India	17
e.	Portugal	17
f.	Australia	18
h.	Thailand	19
i.	Japan	20
III.	Best Practices for E-Government - legal, regulatory and technological measures to protect privacy	21
A.	Privacy Commissioners and Chief Privacy Officers	21
1.	Australia	22
2.	Canada.....	23
3.	Hong Kong	24
4.	New Zealand	25
B.	Privacy Impact Assessments.....	25

1.	What is the goal or purpose of a Privacy Impact Assessment?.....	26
2.	What types of projects warrant PIAs?	27
3.	When should a PIA be performed?.....	27
4.	Who should conduct the PIA?.....	28
5.	What are the outcomes of a PIA?	28
6.	What countries are using PIAs?	29
	a. Canada.....	29
	b. New Zealand	30
	c. United States	30
C.	Privacy Technologies and P3P	30
D.	Privacy Notices.....	31
E.	Privacy Audits	32
	1. What are the elements of a privacy audit?	33
	2. What are the most frequent deficiencies found during privacy audits?.....	34
	3. When should a privacy audit be performed?.....	34
IV.	Emerging Issues	35
	A. Public Records Online – the Court Records Example.....	35
	B. Cybersecurity.....	38
	C. Authentication and Relationship Management	40

Privacy and E-Government

**A Report to the United Nations Department of Economic and Social Affairs
as background for the *World Public Sector Report: E-Government***

by

James X. Dempsey

Paige Anderson

Ari Schwartz

Center for Democracy and Technology

Washington, DC

May 23, 2003

I. Introduction

A. The Importance of Privacy as a Human Right and the Responsibility of the State in Protecting the Privacy of the E-Citizen

Privacy is widely recognized as a human right. Numerous international policy statements and frameworks for the information age declare that individuals are entitled to fair treatment in the way that personal information is collected and used. This includes personally-identifiable information in the hands of government agencies.

Governments are increasingly using the Internet as a means to deliver services and information. This development allows users to register for government services; obtain and file government forms; apply for employment; comment on public policy issues; and engage in a growing number of other functions – all on-line. The trend towards e-government and the electronic delivery of services has further expanded government collection of personally-identifiable data. In providing services to the public and carrying out various functions, governments collect and use a wide range of personal information about their citizens (e.g., health, education, employment and property ownership records, tax returns, law enforcement records, drivers license data, and others). A government's practices in collecting, retaining, and managing personal data about its citizens pose a wide range of privacy concerns. With this increasing use of technology in government-to-citizen interactions, it is important to ensure that government agencies that collect personal information from citizens adopt and maintain adequate privacy practices.

In some ways, the privacy obligations of government information managers are similar to those of businesses that collect customer information. However, governments have special privacy obligations arising from the concept of democracy, which includes the establishment of rules mediating the power relationship between government and citizens. Knowledge is power, and therefore privacy rules are an essential part of the

framework for democracy, for they limit the government's power vis-à-vis the individual represented by control of personal information. In addition, the government's responsibility is heightened because in many respects the government is a monopoly service provider – citizens cannot refuse to deal with the government in the way that they can refuse to deal with merchants who do not respect their privacy.

B. Technology's Impact - Does Technology Redefine the Boundaries of Privacy?

In the Information Age, personal information has become a highly valued commodity that is collected, aggregated, shared and sold in ways never before imagined. Whole industries have formed solely to collect and distribute sensitive information that individuals once viewed as under their control: medical records, personal shopping habits, and financial data. As public institutions move services online, there is growing risk of compromise and abuse. As the US Supreme Court noted, even governmental records that were technically open to public inspection were practically obscure when kept in paper files accessible only with a trip to a central government office. The computerization of records and the linking of dispersed databases, especially through the global Internet, means that records can be accessible anywhere in the world.

At the same time, greater use of information technology does not necessarily mean less privacy. Indeed, technologies can be designed and implemented in ways that enhance privacy. Modern information and communications technologies allow certain interactions to occur at a distance. Whereas face-to-face transactions might entail the disclosure of identity, some on-line interactions can occur anonymously. While it may be hard to keep track of information stored in paper records, automated systems can have built-in audit trails that will detect unauthorized access.

It is certainly true that as the level of technological sophistication rises, so does the level of concern with privacy.

C. Building Citizen Trust in New Government Systems

Trust is a crucial ingredient of any successful 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. Privacy is often cited as a major concern of Internet users; it is also the top reason why many non-users still avoid the Internet.¹ Citizens will not entrust sensitive personal, financial and medical data to the government in order to utilize e-government systems (or they will refuse to give accurate information) unless they are assured that the information will be responsibly used and protected against abuse. Therefore, countries seeking to facilitate the efficient online provision of governmental services must protect the privacy of the information they collect. Government websites and online services should fully comply with the fair information principles outlined below in Section II.B.

¹ See, e.g., World Markets Research Centre, Global E-Government Survey (2001).

To build trust, privacy must be addressed in the planning and design of e-government systems since it is much harder to interject privacy protections after a system is built.

D. Illustrative Case Studies Showing the Ways in Which Privacy Impacts E-Government Practitioners

1. Japan – Juki Net

In August 2002, Japanese citizens took to the streets to protest a new government identification system, called Juki Net. In a society that Westerners sometimes assume does not care about privacy, the project touched a nerve, even prompting several local officials to declare their intent not to cooperate with the national plan. The system's promises of convenience and enhanced security were apparently insufficient to overcome worries about centralization of personal data.

Juki Net is a national ID and information system, based on a database in Tokyo, intended to link a set of personal information consisting of the national 11-digit ID number already assigned to all Japanese citizens, plus name, date of birth, sex, and address. The stated goal of the network, in the short term, is to make it easier for individuals to apply for residency cards from anywhere in the country.

But identity theft is a fast growing crime in Japan. Opponents of Juki Net warned that creating a network that concentrates sensitive information in a single network or location creates a juicy target for identity thieves. There were concerns that civil service workers were not adequately trained to register and protect the information in the database.

Furthermore, Japan has no comprehensive privacy law for the commercial sector. Therefore, there was concern that if the ID number became more centralized and more commonly used, it would be used by commercial entities to collect, store, sell, and combine other information with no notice, consent or access and correction rights afforded the individual.

There were public protests against Juki Net. Protesters wore face paint in the lines of bar codes. Polls indicated that 3 in 4 Japanese citizens opposed the system.

Several major cities backed away from involvement in the project. Yokohama, a city of 3.4 million people, decided to let each resident choose whether to include personal information in the database. The Mayor of Kokubnji held an official "disconnecting" ceremony to show the residents of his city that they would not be included in the database at all.

The Juki Net experience shows that policymakers must address privacy concerns before proceeding to link government databases together. Privacy cannot be an afterthought in the design of information systems. If privacy concerns are not addressed adequately, the result is likely to be public resistance and even non-cooperation.

2. Australia – PKI and Health Records

An example of successful consideration of privacy issues may be Australia's experience in creating a PKI (Public Key Infrastructure) framework to provide authentication and confidentiality for online transactions involving health records. In 2001, the Australian federal Government launched a project to give doctors and hospitals Internet access to patient health records. The project was first introduced to Queensland and Victoria, as a step towards a national electronic patient record.

The system electronically linked general practitioners with other health service providers (hospitals, specialists, pharmacies and others) where each of the service providers and authorized users are equipped with a smartcard. These tools enable the participants to safely communicate with other members of the service network, and ensure that only authenticated users are able to access confidential messages (e.g. patient electronic referrals, discharge notices, pathology test results).

The project included a range of security measures, enabling users to know who sent the message (authentication), that the message content was not been altered in any way between the sender and the receiver (integrity) and that the sender at some stage cannot dispute that they created and sent the message (non-repudiation). It also provided confidentiality by ensuring that only the person to whom the message is directed can open it.

The system incorporated the Information Privacy Principles set out in the Privacy Act. Overall, the design of the system was intended to ensure security and confidentiality of any personal information passed between participating health professionals.²

3. US – Social Security Records Online

In March 1997, the US Social Security Administration set up a Web site intended to allow individuals to obtain their own Personal Earnings and Benefit Estimate Statement (PEBES) over the Internet. To receive a PEBES by email or on a display screen, users were asked to provide their name, social security number, date and place of birth, and mother's maiden name. The SSA program came under intense criticism because it would have been easy for others to obtain illegally the PEBES records over the Internet. On April 9, 1997 the SSA announced that it would suspend the online PEBES service and conduct more research on potential security problems. The system that the SSA came up with in the interim allowed individuals to request their PEBES online, but the report was sent back by paper mail. This was an example of how a failure to address privacy and security in the design of a system generated public distrust and led to the hasty (and embarrassing) redesign of the system.

² See: <http://www.hesa.com.au/>
http://www.hic.gov.au/vendors/security_technology/about_pki.htm

II. Fair Information Practices - Defining Privacy

Of all the human rights in the international catalogue, privacy is often said to be one of the most difficult to define.³ Privacy has been defined as the “right to be left alone” or the “right to control information about oneself.” It has variously been equated with secrecy, confidentiality, anonymity and solitude. The Calcutt Committee in the United Kingdom defined privacy as “The right of the individual to be protected against intrusion into his personal life or affairs, or those of his family, by direct physical means or by publication of information.”⁴ It is clear that definitions of privacy vary widely according to context.

However, in the context of e-government it is not necessary to dwell too long on abstract definitions of privacy, or on the various branches of privacy interests. In the context of e-government, the concept of privacy focuses on “information privacy” (also known as “data protection”). In this context, the notion of being “left alone” is not really relevant. Nor is “privacy” a matter of what is kept secret. Instead, the issue is sometimes characterized as one of control: Individuals should be able to interact with government and provide government agencies with personal information without losing control over subsequent uses of that information. Another way to think of privacy in this context is in terms of “fairness:” When individuals disclose information to the government, that information should be used fairly. In this context, privacy involves the rules governing the collection, use, retention and disclosure of personal information. These rules, sometimes referred to known as “fair information practices,” are discussed in greater detail below.

A. The History of Privacy as a Human Right

It has been said that the recognition of privacy is deeply rooted in history, with references to privacy in the Qur’an, in the sayings of Mohammed, and in the Bible as well as in the laws and culture of classical Greece and ancient China.⁵ Jewish law has long recognized the concept of being free from being watched.⁶

³ James Michael, *Privacy and Human Rights* 1 (UNESCO 1994).

⁴ Report of the Committee on Privacy and Related Matters, Chairman David Calcutt QC, 1990, Cmnd. 1102, London: HMSO, page 7.

⁵ See *Privacy and Human Rights 2002*, EPIC and Privacy International, <http://www.privacyinternational.org/survey/phr2002/>. See also Richard Hixson, *Privacy in a Public Society: Human Rights in Conflict* 3 (1987); Barrington Moore, *Privacy: Studies in Social and Cultural History* (1984).

⁶ See Jeffrey Rosen, *The Unwanted Gaze* (Random House 2000).

In some respects, the first modern privacy law was adopted in 1766, when the Swedish Parliament enacted the Freedom of Press Act, requiring that all government-held information be used for legitimate purposes and granting citizens the right to access government data held about themselves. The Swedish law still remains an international model.

A modern privacy benchmark at an international level can be found in the 1948 Universal Declaration of Human Rights,⁷ Article 12 of which states:

No one should be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks on his honour or reputation. Everyone has the right to the protection of the law against such interferences or attacks.

Various other international human rights instruments specifically recognize privacy as a right. Article 17 of the International Covenant on Civil and Political Rights (ICCPR), Article 14 of the UN Convention on Migrant Workers, and Article 16 of the UN Convention on Protection of the Child all recognize and protect some aspect of the right to privacy.⁸

On the regional level, various treaties make these rights legally enforceable. Article 8 of the European Convention for the Protection of Human Rights and Fundamental Freedoms⁹ states:

(1) Everyone has the right to respect for his private and family life, his home and his correspondence. (2) There shall be no interference by a public authority with the exercise of this right except as in accordance with the law and is necessary in a democratic society in the interests of national

⁷ Universal Declaration of Human Rights, adopted and proclaimed by General Assembly resolution 217 A (III) of December 10, 1948, available at <http://www.un.org/Overview/rights.html>.

⁸ International Covenant on Civil and Political Rights, adopted and opened for signature, ratification and accession by General Assembly resolution 2200A (XXI) of December 16, 1966, entry into force March 23 1976, available at http://www.unhchr.ch/html/menu3/b/a_ccpr.htm; International Convention on the Protection of the Rights of All Migrant Workers and Members of Their Families, adopted by General Assembly resolution 45/158 of December 18, 1990, available at http://www.unhchr.ch/html/menu3/b/m_mwctoc.htm; Convention on the Rights of the Child, General Assembly resolution 44/25 of November 20, 1989, entry into force September 2, 1990, available at <http://www.unhchr.ch/html/menu3/b/k2crc.htm>.

⁹ Council of Europe, Convention for the Protection of Human Rights and Fundamental Freedoms, (ETS no: 005) 1950, <http://conventions.coe.int/Treaty/EN/cadreprincipal.htm>.

security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health of morals, or for the protection of the rights and freedoms of others.

The Convention created the European Commission of Human Rights and the European Court of Human Rights to oversee enforcement. Both have been active in the enforcement of privacy rights. In particular, the Court has reviewed cases of individuals' access to their personal information in government files to ensure that adequate protections are followed.¹⁰

The concept of information privacy as a human right in the context of government data is especially fully developed in Latin America. Article 11 of the American Convention on Human Rights sets out the right to privacy in terms similar to the Universal Declaration.¹¹ In the efforts of Latin America to establish and strengthen constitutional democracies, a fundamental consideration has been the right of access to state-held information. One means of guaranteeing the right to protection against information that is abusive, inaccurate, or prejudicial to individuals is through access to public databases for the purpose, as necessary, of updating, correcting, removing, or reserving information about the individual concerned. This action is known as *habeas data*. Principle 3 of the IACHR Declaration of Principles on Freedom of Expression provides:

Every person has the right to access to information about himself or herself or his/her assets expeditiously and not onerously, whether it be contained in databases or public or private registries, and if necessary to update it, correct it and/or amend it.

The OAS's Special Rapporteur for Freedom of Expression has said that the action of *habeas data* is based on three premises: (1) the right of every individual to undisturbed privacy, as reflected in Article 11 of the Convention; (2) the right of every individual to obtain access to information about him in public and private databases in order to modify, remove, or correct sensitive, false, biased, or discriminatory information about him; and (3) the right of individuals to resort to the action of *habeas data* as an enforcement mechanism. This right of access to and control over personal data represents a fundamental right in many aspects of life, since the lack of judicial mechanisms for the rectification, updating, or removal of data would directly affect the right to privacy, honor, individual identity, property, and accountability in the collection of data.¹² The Special Rapporteur has noted:

¹⁰ Judgement of 26 March 1987 (Leander Case).

¹¹ Signed November 22, 1969, entered into force July 18, 1978, O.A.S. Treaty Series No. 36, at 1, O.A.S. Off. Rec. OEA/Ser. L/V/II.23 dec rev. 2, available at <http://www.oas.org/juridico/english/Treaties/b-32.htm>.

¹² Report of the Special Rapporteur for Freedom of Expression, Chapter III,

The action of *habeas data* takes on even greater importance with the introduction of new technologies. Through greater use of computers and the Internet, both the state and the private sector have rapid access to vast amounts of personal data. It is therefore necessary to ensure that concrete channels exist to provide rapid access to information for the purpose of modifying inaccurate or outdated information contained in electronic databases, protecting the right to individual privacy.¹³

The African [Banjul] Charter on Human and Peoples' Rights, adopted June 27, 1981, does not expressly mention the right of privacy.¹⁴ There is no regional human rights treaty for Asia. Nevertheless, as noted below in Sections II.C and II.D, there is growing attention to privacy in Asia and, to a lesser extent, in Africa

B. The COE/OECD/EU Principles

At the beginning of the computer revolution, governments developed a set of Principles of Fair Information Practices. The Principles are intended to foster individuals' control over their personal information, limit data collection, and place responsibilities on data collectors. These Principles are the basis for most modern data protection and online privacy laws and policies.

The principles of "fair information practices" are embodied in two highly influential international instruments, both adopted in 1981: the Council of Europe (COE) Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data ("COE Convention") and the Organization for Economic Cooperation and Development (OECD) Guidelines Governing the Protection of Privacy and Transborder Data Flows of Personal Data ("OECD Guidelines").¹⁵ Both instruments articulate a

Report on Action with Respect to *Habeas Data* and the Right of Access to Information in the Hemisphere,
<http://www.cidh.org/relatoria/english/annualreports/ar01/chapteriii2001.htm>

¹³ Id.

¹⁴ <http://www1.umn.edu/humanrts/instreet/z1afchar.htm>.

¹⁵ 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>. The COE/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. The basic principles of the 1973 U.S. Department of Health, Education & Welfare (HEW) Code are as follows:

similar set of principles regarding the handling of personal data – principles that 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.¹⁶

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

-
- There must be no personal data record-keeping systems whose very existence is secret;
 - There must be a way for an individual to find out what information is in his or her file and how the information is being used;
 - There must be a way for an individual to correct information in his or her records;
 - Any organization creating, maintaining, using, or disseminating records of personally identifiable information must assure the reliability of the data for its intended use and must take precautions to prevent misuse; and
 - There must be a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without his or her consent.

¹⁶ To date, over twenty countries have adopted the COE Convention and another six have signed it but not adopted it into law. In addition to being relied upon by OECD nations to create data protection laws, the OECD Guidelines have been relied upon by other nations that are not OECD members. For example, Hong Kong, Estonia, and Lithuania seem to have based their privacy laws, in part, on the OECD Guidelines. Brazil and Malaysia are currently considering passage of privacy laws based on the OECD Guidelines. Jeffrey B. Ritter, Benjamin S. Hayes, Henry L. Judy, Emerging Trends in International Privacy Law, *Emory International Law Review*, vol. 15, p. 87, 92. See also UN Guidelines for the Regulation of Computerized Personal Data Files (1990). An excellent summary of these principles is found in "National Privacy Principles," issued by the Office of the Federal Privacy Commissioner, Australia, <http://www.privacy.gov.au/publications/npps01.html>.

“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.
- **Access [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 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.¹⁷

C. Is Privacy Culturally Determined or International?

The question of whether privacy is a concept limited to “Western” cultures has now been resolved by the adoption of privacy laws in countries around the world – countries with such disparate cultures as Argentina, South Africa, Japan and Thailand have adopted privacy laws governing public and/or private databases, and the principles in those laws are similar to the principles in the guidelines of the OECD.¹⁸

¹⁷ “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.

¹⁸ Others have noted that, across the emerging body of global privacy law, general patterns are beginning to emerge. Jeffrey B. Ritter, Benjamin S. Hayes, Henry L. Judy, *Emerging Trends in International Privacy Law*, *Emory International Law Review*, vol. 15, p. 87, 88.

On a sociological or philosophical level, there is support for the proposition that some basic concept of privacy is nearly universal. Stanley Benn, for example, while conceding that there is great diversity among different cultures in both the form and substance of privacy concepts, nevertheless concluded that privacy in its most basic form represents a necessary consequence of human existence. In particular, Benn argues that “some minimal right to immunity from uninvited observation and reporting is required by certain basic features of our conception of a person.”¹⁹ Similarly, Alan Westin concluded based on a survey of cultural data that certain privacy-related features appear to be cross-cultural constants. Westin's observations seem to suggest that at least some fundamental, rudimentary aspects of privacy form an integral part of social life, preserving both the individual's separateness from society and his existence within it. Some non-Western societies display behaviors that may be seen as intensely private. For example, the use of the veil by women in Islamic cultures can be regarded as an expression of privacy (among other complex and deeply held values).

Regardless of these philosophical and sociological considerations, there are important trends underway worldwide that have brought with them a concern about privacy in otherwise very diverse cultures. One factor contributing to the emergence of a global conception of privacy may be the impact of cyberspace itself. Under this view, the Internet is not merely a technological innovation facilitating global communication but also a cultural sphere characterized by distinct social values and rules. As the Internet culture spreads to developing countries, it brings with it a certain set of values that include user control over information.²⁰

Secondly, privacy seems to be a component of democracy. The development of democracy concerns how much power the government has, and whether it exercises that power arbitrarily or subject to rules that respect the control of the individual. If knowledge is power, and if democracy is about giving power to individuals, then the development of democracy carries with it the concept of information privacy, which concerns guaranteeing that the individual citizen has the power to control disclosure of information to the government and the subsequent use by the government of that information. Concern with information privacy, especially in the context of government databases, grows with the progress of democratization. There seems to be evidence that legal protection of privacy accompanies the development of democracy, across otherwise

¹⁹ Stanley I. Benn, Privacy, Freedom, and Respect for Persons, in Privacy, Nomos XIII, supra note 11, at 1, 3. See Alan Westin, The Origins of Modern Claims to Privacy, (a comprehensive, world-wide compilation of cultural data) in Philosophical Dimensions of Privacy, 56, 60-61 (Ferdinand David Schoeman, ed. 1984) hereinafter Philosophical Dimensions.

²⁰ Katrin Schatz Byford, Privacy In Cyberspace: Constructing A Model Of Privacy For The Electronic Communications Environment, Rutgers Computer and Technology Law Journal, vol. 24, p. 1 (1998).

diverse cultures. The defining characteristic of countries that do not respect privacy may therefore not be cultural, but political.²¹

The third powerful driver of the development of privacy law has been the desire of developing countries to engage in global e-commerce and the recognition that trust is a fundamental component of e-commerce. Accompanying this has been the impact of the EU Data Protection Directive, which prohibits disclosure of data from EU Member States to countries that do provide adequate privacy protection.

For these and other reasons, concern with privacy is manifesting itself in public policy discussions around the world. For example, the Asia Pacific Economic Cooperation (APEC) group held a conference in Thailand, February 13, 2003 entitled "Addressing Privacy Protection: Charting a Path for APEC." The conference brought privacy advocates, businesses and government representatives together to develop a new approach to online data privacy for the Asia-Pacific Region. Executive Director of the APEC Secretariat, Ambassador Piamsak Milintachinda, said "This conference highlights the importance of data privacy as an important policy aspect of the burgeoning e-commerce industry in the Asia-Pacific."²²

In Africa, too, there are growing signs of interest in privacy. For example, in a closing declaration at the Africa Regional INFOethics Workshop, Addis Ababa, Ethiopia, September 13-14, 2000, participants recommended that basic human rights be preserved in the dissemination of information through the application of new ICTs by continuously striving for a balance between the fundamental rights for freedom of expression and the equally important rights for privacy. The conference participants declared that the African public and private sectors should ensure that personal information generated for one purpose is not used or disclosed for another without the knowledge and consent of the person concerned. They called upon nations of Africa to establish privacy protection acts, based on wide consensus, taking into account the interests of the citizens as well as business for confidentiality.²³

²¹ Id.

²²

http://www.apecsec.org.sg/whatsnew/press/PressRel_PrivProtctnOvercomeConFear_110203.html.

²³ Conclusions of the Africa Regional INFOethics Workshop, Addis Ababa, Ethiopia, September 13-14, 2000

http://webworld.unesco.org/infoethics2000/documents/rec_ethiopia.rtf

D. Examples of Government Records Privacy Law Around the World

Many countries have adopted national privacy or data protection laws.²⁴ 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 laws applicable to government databases, but the privacy principles are actually the same for both commercial and governmental data.

1. Overview

In the Asia Pacific region, the following countries have data protection and privacy laws: Australia, China, Hong Kong, India, Japan, South Korea, Malaysia, New Zealand, the Philippines, Singapore, Taiwan and Thailand. To some extent, the activity in Asia is prompted by a desire to improve electronic commerce and ensure that data flows with Europe will not be interrupted by the EU Directive, but there are also laws specifically focusing on privacy of government databases. The OECD guidelines have also played an important role in the development of Asian privacy laws. Hong Kong and New Zealand have comprehensive acts in force. Taiwan's act covers the public sector and eight areas of the private sector. Japan's law protects information held in government computers. South Korea's law is limited to the public sector (except for a separate law on credit reports).

In Central and South America, data protection laws have been adopted in Argentina, Chile, Brazil and Peru. A number of Latin American countries (including Argentina, Brazil, Dominican Republic, Paraguay, Peru and Venezuela) have incorporated the right of habeas data (access to data) into their constitutions. Several countries have moved towards adopting data protection laws to give force to this right. There is also interest in the region in ensuring trade with Europe. Recently, a comprehensive data protection law was adopted in Argentina based on the EU Directive. Several other countries including Paraguay and Chile have more limited habeas data laws allowing access and correction rights. In March 2002, Peru created a Commission to draft a more comprehensive law.

In Central and Eastern Europe, in response to the repression of the Soviet era and as the process of accession to the EU moves forward rights of privacy have been enshrined in a number of countries' constitutions. Examples include Hungary and Lithuania.²⁵ In Bulgaria, a new Personal Data Protection Act came into effect in January

²⁴ For an international survey of privacy law, including country-by-country reports, see *Privacy and Human Rights 2002*, EPIC and Privacy International, <http://www.privacyinternational.org/survey/phr2002/>

²⁵ Jeffrey B. Ritter, Benjamin S. Hayes, Henry L. Judy, *Emerging Trends in International Privacy Law*, *Emory International Law Review*, vol. 15, p. 87, 104

2002. In Estonia, the Government drafted amendments to the Data Protection Act to bring it into full compliance with the EU Data Protection Directive. Poland ratified the Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data (ETS No. 108) in May 2002. In 2001, Slovenia amended its Data Protection Act in order to establish an independent supervisory authority.

The Middle East countries have not implemented extensive privacy or data protection laws. Only Israel has adopted comprehensive legislation protecting privacy. Some data protection legislation exists in Jordan. There is also little advancement towards privacy laws in Africa. Only in South Africa has there been an effort to provide for data protection. Other countries including Uganda and Namibia have recently debated adopting freedom of information acts, which would presumably allow individuals access to their own records held by government agencies.²⁶

2. Selected Examples

Some of the following public records privacy protections are part of broader personal data protection legislation, prompted by commercial needs to provide greater protections for personal data. There are several countries, though, that do have separate regulations specifically addressing the government's handling of personally identifiable information.

Common elements in the protections include: (1) limiting the collection of personal information to specific purposes; (2) requiring some type of consent for collection and disclosure of the information; and (3) exempting databases pertaining to crime, security, or national archives. The majority of the public records protections include a balance between protecting individual rights to privacy, the public benefit of free information exchange, and the state's interest in protecting national security. While the existence and format of public records data protections vary, it is clear that there is a deep trend worldwide toward pushing public sector protections forward.

a. Republic of South Africa

The *Promotion of Access to Information Act of 2000* is intended to give citizens access to information in the hands of the government. Several provisions in the law touch on the tension between openness and privacy protection. In general, the Act sets the rule that disclosure of personally identifiable information is to be refused when it would represent an unreasonable disclosure of personal information of a third party. The Act explains that disclosure is acceptable when: (1) an individual has given permission that the information be disclosed to the requester; (2) the individual to whom the information pertains was made aware that it would be made public; (3) the information is already publicly available; (4) the information concerns the physical or mental well-being of an individual under 18 years old or incapable of understanding the request, and the requester is a care giver; (5) the information is about a deceased individual when

²⁶ Id.

requester is next of kin, or the request is made with the consent of the next of kin; or (6) the information is about a public official and the information requested relates to his or her public role. Another exception provides that a public officer must disclose personal information held by the government agency, even if the disclosure violates another provision of the Act, when (i) such disclosure would reveal evidence of law-breaking, an imminent and serious public safety or environmental threat, and (ii) the public interest served clearly outweighs the invasion of personal privacy. The Act also contains special protections for the records of the South African Revenue Service, mandating that no records from that agency be released if the records contain information obtained for the purposes of revenue collection.²⁷

b. Hong Kong

Hong Kong adopted its Personal Data Privacy Ordinance in 1996. The Ordinance contains six principles governing the collection, storage and dissemination of personal data by both public and private sectors. Personally identifiable information can only be collected for a specified purpose and utilized for that purpose only or a directly related purpose. Any individual has the right to inquire whether a data holder possesses personal data about themselves and to have access to that data, unless release poses a danger to national security.²⁸ Data requests can be denied if the request is too general or follows two or more requests by, or on behalf of, the same individual.

In 1995, the government also passed a Code on Access to Information to guide government entities in managing information. Included in the Code is a section on the privacy of personal information held by the government. Specifically, Section 2.15.1 of the Code limits access to personal information held by the government to instances when (a) disclosure is consistent with the purposes for which the information was collected; (b) the subject of the information, or other appropriate person, has given consent to its disclosure; (c) disclosure is authorized by law; and (d) the public interest in disclosure outweighs any harm or prejudice that would result.²⁹ The restriction on releasing personal information does not apply to information from which an individual is not easily identifiable. The Code protects the privacy of all information held by the government regardless of whether it is categorized as confidential.³⁰ The Code does not apply to information held by courts and tribunals.

²⁷ Promotion of Access to Information Act of 2000, Government of South Africa, <http://www.gov.za/gazette/acts/2000/a2-00.pdf>.

²⁸ Office of the Privacy Commissioner for Personal Data, Hong Kong, http://www.pco.org.hk/english/ordinance/section_30.html.

²⁹ Hong Kong Government, Code of Access to Information, http://www.info.gov.hk/access/guide.htm#para2_15.

³⁰ Id. at 2.15.9.

Hong Kong has a highly developed e-government system which allows citizens to pay taxes, renew driving licenses, register to vote, and search government information online.³¹ Hong Kong is also implementing a new Smart Identification card for all citizens in July 2003. All cards will be embedded with personal information, a photograph, and both thumbprints. For non-permanent residents information regarding length of stay is included. Citizens will also have the choice of embedding the card with value-added applications such as a digital certificate, library card, change of address functions, and driver's license. All information that is stored on the card can be viewed at self-serve kiosks. To protect the privacy of personal information held on the card, there will be no sharing of that information between government agencies, and the information will not be held on one central database.³²

c. Canada

Canada's federal Privacy Act of 1982 regulates the government's collection, retention, and dissemination of personal information. The Act provides access for individuals and the private sector to government records and outlines fair information practices intended to protect personal information. Information requests are made to the particular government agency with which the information resides. The general protection provisions can be overruled by any other federal legislation that explicitly allows access to that personal information.

The Privacy Act states that personal information held by the government cannot be used by the government except for the purpose for which the information was obtained or for a use consistent with that purpose. The two main exceptions to the Act are disclosures allowed (1) under any other act of Parliament or regulations created to carry out those Acts, and (2) by consent of the individual to whom the information pertains. Some examples of allowable disclosures are subpoenaed information to law enforcement agencies, research purposes, and any purpose where the head of the agency holding the information deems disclosure to benefit the public more than the invasion to the individual's privacy.³³

Until May 2000, the Human Resources Development office maintained a central database with personal information about all Canadian citizens, called the Longitudinal Labor Force File. The database contained information from tax returns, benefits and

³¹ Hong Kong E-Government Site, <http://www.info.gov.hk/digital21/e-gov/eng/init/esd.htm>.

³² Hong Kong Government Smart Identity Card, <http://www.info.gov.hk/immd/english/idcard/main.htm>.

³³ Canadian Privacy Act of 1982, Section 7- 8, http://www.privcom.gc.ca/legislation/02_07_01_e.asp#005.

welfare files, and social insurance files. The database was dismantled after a report filed by Canada's Privacy Commissioner.³⁴

d. India

India's *Freedom of Information Act of 2002* limits access to personal information held by the government when the request for information: (1) is too general; (2) relates to information that is going to be published pursuant to a law within thirty days of receipt of the request, or has been published in a public document previously; or (3) relates to information that would cause unwarranted invasion of an individual's privacy.³⁵ The law's provisions apply exclusively to government bodies and any organizations directly or indirectly funded by the government. Section 16 of the Act exempts national intelligence agencies, citing security concerns. When the government discloses personal information, written notice is sent to the individual whose information was disclosed within twenty-five days of when the request for the information was received.³⁶ The law has been criticized for its broad exemptions, insulating government communications from disclosure. It has also been criticized because when an information disclosure request is denied, all appeals are handled within the government. There is no access to an independent authority for appeal.³⁷

e. Portugal

Portugal's *Act on the Protection of Personal Data* is modeled on the European Union's 1995 Directive on Data Protection. Specifically the Act provides broad access for an individual to government information held about that individual, and the right to ensure its accuracy. The National Data Protection Commission monitors compliance with the Act. An individual's personal data can only be collected and stored: (1) with express authorization by the individual; (2) for the performance of a contract to which the data subject is a party; (3) for compliance with a legal obligation; (4) to protect the vital interests of the data subject if he is incapable of giving consent; and (5) for performance

³⁴ Minister of Human Resources Development Canada, HRDC Dismantles Longitudinal Labour Force File Databank, May 29, 2000, www.hrdc-drhc.gc.ca/common/news/dept/00-39.shtml.

³⁵ Indian Legislature, Freedom of Information Act of 2002, Section 9, <http://indiacode.nic.in/cgi/nph-bwcgi/BASIS/indweb/all/iw2/DDW?W%3DSECTEXT%20%20PH%20IS%20%27privacy%27%26M%3D7%26K%3D39466%26U%3D1>.

³⁶ Section 11(1), Freedom of Information Law, <http://www.freedominfo.org/news/india/foi2002.doc>.

³⁷ Prashant Bhushan, India Approves Freedom of Information Law, December 2002, < <http://www.freedominfo.org/news/india/>>.

of an act carried out in the public interest where such performance does not violate an individual's fundamental personal rights. In Article Seven, the law also provides express protection for sensitive data, defined as data pertaining to philosophical or political beliefs, political party or trade union membership, religion, privacy and racial or ethnic origin, and health or sex life, and genetic data. Sensitive data can be collected in limited circumstances if the data subject provides express consent or if such collection is in the best interest of the public or the data subject themselves.³⁸ Databases containing information about individuals' criminal activity may only collect, store, or transfer personal information when doing so is necessary to prevent a "specific danger or prosecute a particular offense."³⁹ Data subjects are provided notice by the government that personal data has been collected (unless the collection is for statistical research of State security). Individuals have the right to object to the processing of their personal information and the processing will cease unless there is an overriding public interest or third party interest in the processing of that data.⁴⁰ The law also protects an individual's data from being transferred to a state outside the European Union unless that state has comparable data protection laws.

f. Australia

Under the *Privacy Act of 1988*, Australia's government agencies are required to comply with eleven Information Privacy Principles to ensure the secure storage of personal information. There are also separate provisions governing the use of tax file numbers and health information. Principle Nine explains that personal information shall be used only for a purpose to which the information is relevant. On disclosure of personal information, Principle Ten states that information shall not be used for any other purpose except when (a) the individual concerned has consented to use of the information for that other purpose; (b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person; (c) use of the information for that other purpose is required or authorized by or under law; (d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or (e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.⁴¹ Principle 11 addresses limits on the disclosure of personal information to any third party, including another government agency. Specifically, information cannot be disclosed unless: (i) the individual concerned is reasonably likely to have been aware, or made aware that information of

³⁸ [Act on the Protection of Personal Data, 1998,](http://www.cnpd.pt/Leis/lei_6798en.htm)
http://www.cnpd.pt/Leis/lei_6798en.htm.

³⁹ *Id.* at Article 8.

⁴⁰ *Id.* at Article 12.

⁴¹ Office of the Federal Privacy Commissioner, Australia,
< <http://www.privacy.gov.au/publications/ipps.html#f>>.

that kind is usually passed to that person, body or agency; (ii) the individual concerned has consented to the disclosure; (iii) the record-keeper believes on reasonable grounds that the disclosure is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or of another person; (iv) the disclosure is required or authorized by or under law; or (v) the disclosure is reasonably necessary for the enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue.⁴² When personal information is disclosed for law enforcement or public revenue purposes, a note is made on the individual's record.

g. Argentina

In Argentina, the *Personal Data Protection Act*, based on the European Union Data Protection Directive, applies to both public and private databases. Journalistic information sources or databases are exempted. All databases must be registered. Chapter one, section four requires that data only be used for the purposes for which it was collected, and must be destroyed once the purposes for which it was collected have ended. Individuals must give express consent in writing for their personal information to be collected, stored or transferred. Consent is not necessary when the data is collected from a public-access database or by the State in "performance of duties inherent in the powers of the State, or consists only of name, national identity card number, taxing or social security identification, occupation, date of birth, domicile and telephone number."⁴³ Individuals are afforded special protection regarding "sensitive data" relating to racial or ethnic backgrounds. No individual can be compelled to provide such information and any information that is collected must be for scientific studies and cannot be identifiable. Although consent is required before personal data can be transferred, government agencies are permitted to share personal data without consent or notification of the subject.⁴⁴

Individuals have a right of habeas data to access information about themselves that is held by the government and private entities. The law is administered by an independent commission within the Ministry of Justice.

h. Thailand

The legal basis for information access and privacy protection in Thailand is the Official Information Act of B.E. 2540 (OIA),⁴⁵ a product of the recent political reform movement in Thailand. The act came into force in September 1997 just a month before the proclamation of the present Constitution and provides the legal basis for the "Right to Know" and the "Right to Privacy." Section 4 of the Official Information Act defines "Personal Information" as information relating to all the particular private matters of a

⁴² Id.

⁴³ <http://www.ulpiano.com/Dataprotection_argentina.htm>

⁴⁴ Id at Section 11.

⁴⁵ <http://www.oic.thaigov.go.th/eng/statue/statue.htm>.

person which contain indications identifying that person. Such personal information includes, for instance, educational, financial, health, criminal history and employment records, which contain the name of such person or a numeric reference, code or such other indications identifying that person as fingerprint or photograph. All State agencies are obliged by law to provide proper protection for this information.⁴⁶

All State agencies are obliged to provide an appropriate security system for the personal information system (Section 23 (5)). The dissemination or disclosure of personal information held by a State agency - without consent of its subject - is restricted by the Act. In general, dissemination without consent of the information subject is only permissible where it is necessary to serve a higher public or private interest or justified by law (Section 24).

If, for example, a married couple reveals their financial information to the Court for purposes of a divorce process, this information can be used only for this purpose - and not, for example, disseminated to the tax authorities. The same applies to the information of farmers given to the Bank for Cooperation and Agriculture. Personal information collected for purposes of a loan agreement should not be transferred or disclosed to the tax authorities.

A further goal of the Act is to make data processing in State agencies open, correct, accessible, reviewable and subject to supervision and auditing. State agencies are not normally allowed to collect information without notice. State agencies are obliged to inform the data subject about the collection of such personal information. It must be possible for the person affected to access and monitor the path they take and review its content (Section 25).

i. Japan

The Law for the Protection of Computer Processed Personal Data Held by Administrative Organs was enacted in December 1988. It was enacted in conformity with the OECD Guidelines of 1980 and provides for the protection of data which is processed using computers owned by the administrative organs of the government. The law covers all data held by the public sector.

Under the law, prior notification to the Director General of the Management Coordinator Agency is required for any national administrative organs holding, modifying or disclosing of personal data. Any organ which has notified the Management and Coordinator Agency must compile a directory of all personal file holdings and make it accessible to the public. Exceptions to this general rule exist, for example, for files

⁴⁶ Kittisak Prokati(Thammasat University), Information Access and Privacy Protection in Thailand, paper presented at the Conference on Freedom of Information and Civil Society in Asia held by Information Clearinghouse Japan in 13-14 April 2001, <http://www.foi-asia.org/Thailand/KPreport.html>.

recording matters concerning the security of State. Also, file controllers do not need to register files if notification might disrupt important administrative functions such as investigation and prevention of crime.

III. Best Practices for E-Government - legal, regulatory and technological measures to protect privacy

A. Privacy Commissioners and Chief Privacy Officers

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.⁴⁷

Colin Bennett, professor of political science at the University of Victoria (Canada) has identified eight inter-related roles that data commissioners play: ombudsman, auditor, consultant, educator, policy advisor, negotiator, enforcer, and international ambassador.

Most of the privacy commissioners are in member countries of the European Union. Under Article 28 of the European Union Data Protection Directive,⁴⁸ 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

⁴⁷ 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.

⁴⁸ 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.

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 the power to conduct investigations, oversight and enforcement. Ontario Privacy Commissioner Ann Cavoukian stresses her ability to undertake privacy investigations in both the private and public sectors as an important tool in her daily work. Even when the law does not enable commissioners to fine companies or agencies, the public spotlight from such investigations is enough to shame organizations into doing the right thing.

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. The most effective privacy commissioners head independent agencies. Their independence affords them the ability to take positions different from those of the legislature and executive branch and even speak openly to the legislature or media about these differences. To most privacy commissioners, this independence is the agency's greatest asset and power. For example, Australia Privacy Commissioner Malcolm Crompton sees his ability to criticize the government in the media as central to his mission.

Finally, privacy commissioners need resources. The Dutch Privacy Office has a staff of more than 50 for a country of 15 million.

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

1. Australia

Australia's Office of the Federal Privacy Commissioner is tasked with creating a culture "in which privacy is respected, promoted and protected."⁴⁹ 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.⁵⁰ The Office of the Federal Privacy Commissioner has specific authority to:

- Investigate complaints from individuals about potential interference with their privacy;

⁴⁹ 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/

⁵⁰ *Privacy and Human Rights 2002*, EPIC and Privacy International, at 105.

- 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.

2. 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.⁵¹ The Commissioner has authority to:

- Publish information about personal information handling 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.⁵² Ideally, complaints are resolved through negotiation, mediation and

⁵¹ http://www.privcom.gc.ca/faq/faq_01_e.asp#002.

⁵² See http://www.privcom.gc.ca/au_e.asp.

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.⁵³

Privacy commissioners also have been established at the provincial level to oversee the implementation of privacy-related legislation adopted by provincial governments.⁵⁴ 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.⁵⁵

3. Hong Kong

In Hong Kong, the Personal Data Ordinance establishes a privacy oversight entity, the Office of the Privacy Commissioner for Personal Data, which is tasked with promoting and enforcing compliance with the statutory requirements in the Ordinance.⁵⁶ 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.

⁵³ Id.

⁵⁴ See e.g., http://www.ipc.on.ca/scripts/index_.asp?action+31&N_ID=17&U_ID=0.

⁵⁵ Privacy and Human Rights at 143.

⁵⁶ <http://www.pco.org.hk/>

4. 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.

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.⁵⁷

B. Privacy Impact Assessments

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."⁵⁸ 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

⁵⁷ Annual Report of the Privacy Commissioner for the year ended 30 June 2002, at 11, available at <http://www.privacy.org.nz>.

⁵⁸ 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 Privacy Commissioner for New Zealand, is one of the main originators of the concept of the PIA.

recommends changes in the technology or policies in order to avoid or mitigate the adverse effects on privacy.⁵⁹

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.⁶⁰

1. 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

⁵⁹ Ontario Province, Canada has created a Privacy Impact Assessment toolkit, meant to educate governments interested in evaluating their information collection policies against widely-accepted privacy criteria. <http://www.gov.on.ca/MBS/english/fip/pia>.

⁶⁰ For example, the Office of the Privacy Commissioner in New Zealand notes that both national and international privacy standards are relevant to PIAs. 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>

course of their decision-making on a particular project or program that will involve data collection.

2. 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:

- 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.⁶¹

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.

3. 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

⁶¹ See *Privacy Impact Assessment Guidelines*, Freedom of Information and Privacy Office, Management Board Secretariat, Ontario, Canada (June 2001) <http://www.gov.on.ca/MBS/english/fip/pia/index.html>; *Privacy Impact Assessment, PIA: Some Approaches, Issues and Examples*, presentation by Blair Stewart, Assistant Privacy Commissioner, New Zealand, available at <http://www.pco.org.hk/misc/stewart/tsld001.htm>

meaningful, the PIA should 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.

4. 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.

5. 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.⁶² 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.)

⁶² 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*, by 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>.

- 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.⁶³ 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.

6. 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.

a. 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.⁶⁴ 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.⁶⁵ PIAs are made available on public websites.

⁶³ Canada, for example, requires PIAs to be posted on the Internet. New Zealand also requires the public release of these materials.

⁶⁴ 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.

⁶⁵ *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,

b. 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>.

c. 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.⁶⁶

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 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.

C. Privacy Technologies and P3P

Technology itself can be designed in such ways as to better protect privacy. One of the technological innovations is the Platform for Privacy Preferences (P3P). P3P is essentially a common language for expressing Web site privacy policies in machine-readable form. It allows users to set their Web browsers to automatically read Web site privacy policies and match them against a user's own preferences. P3P is designed to provide Internet users with a clear understanding of how personal information will be used by a particular Web site, upfront, without having to read small-print legalese. These tools can display information about a site's privacy policy to end users and take actions based on a user's preferences. Such tools can notify users when the sites they visit have privacy policies matching their preferences and provide warnings when a mismatch occurs. Web site operators can use the P3P language to explain their privacy practices to visitors. Users can configure their browsers or other software tools to provide notifications about whether Web site privacy policies match their preferences. Parents can set privacy rules that govern their children's activities online. Consumers can make better judgments about which Web sites respect their privacy concerns.

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.

⁶⁶ Links to the text and legislative history of the E-Government Act are available at: <http://www.cdt.org/legislation/107th/e-gov/>.

P3P is not a panacea for privacy, but it does represent an important opportunity to make progress in building greater privacy protections in the Web experience of the average user.⁶⁷ In the US, federal government websites are beginning to use P3P.

D. Privacy Notices

Notice is the act of informing individuals that personal information about them is being collected; how it will be used, stored and disclosed; and how long the information will be retained. Posting privacy policies is essential in building trust between Web sites and their users; policies are created to inform users of a site's data collection, use and disclosure practices. A good policy should be based on the fair information practices set forth in the OECD Guidelines and other compilations of privacy principles. Once created, the policy should be posted online with prominent links from pages where data is collected. While privacy notices do not in and of themselves guarantee privacy protection, they offer a basis for public and legislative scrutiny of agency practices.⁶⁸

Notice gives Web site visitors sufficient information to decide if they want to: proceed with providing their personal information on-line; use another method for submitting their personal information (such as the phone or in-person); or opt out entirely. The Canadian Government puts it this way:

Privacy Notice Statements serve the purpose of building trust and confidence in Government of Canada Web sites. This is important to the success of the Government's GOL initiative (Government On-Line) in which programs and services are increasingly made accessible on-line. A number of Canadians have become suspicious of the Internet in general. News stories about hackers, unscrupulous operators and Web sites that share personal information without seeking permission, have all contributed to reluctance on the part of some people to submit information on-line. Privacy Notice Statements help illustrate that Government of Canada Web sites are trustworthy.⁶⁹

⁶⁷ The P3P Specification, the W3C announcement and a wealth of other information may be viewed at <http://www.w3c.org/P3P/#news>. For more information on P3P, see "P3P and Privacy: An Update for the Privacy Community," by CDT and the Ontario Information and Privacy Commissioner:

<http://www.cdt.org/privacy/pet/p3pprivacy.shtml>.

The P3P home page is <http://www.w3c.org/p3p/>. Other helpful assistance may be found at <http://www.p3ptoolbox.org>.

⁶⁸ OMB Memorandum M-99-18, Privacy Policies on Government Web Sites, <http://www.whitehouse.gov/omb/memorandum/m99-18.html>

⁶⁹ http://www.cio-dpi.gc.ca/pgol-pged/nandc-aetc/nandc-aetc03_e.asp.

Model privacy notices have been developed.⁷⁰ Here is a short set of questions that should be answered in a privacy policy:

- What information is being collected? Is the information personally identifiable?
- Why is it necessary to collect this information? Is the data collection appropriate to the activity or transaction? If not, why does the site need it?
- How is the data being collected? Does the site set cookies? Does the site maintain web logs?
- How is personal information used once it is collected? Is it ever used for purposes other than those for which a visitor has provided it? (If so, the visitor should be informed of the use.) Has the visitor consented to it? Does the visitor have the option to prohibit such secondary use? Can a visitor prohibit it and still enjoy the site?
- Does the site offer different kinds of service depending on user privacy preferences? Does a user have a choice regarding the type and quantity of personal information that the site collects? Does the site disadvantage users who exercise data collection choices?
- Can users access information that has been collected about them? Are users able to correct inaccurate data?
- How long is personal information stored? Is it kept any longer than necessary for the task at hand?
- What is the complaint and redress process? Whom can users contact?
- What laws govern the collection?

While some sites will need to go into highly specific detail on one or more questions, a good starting point is a short, easy to read set of answers with links to more specific information (e.g. descriptions of technical information in web logs, links to governing laws), which enables a user to get a general idea without having to read through legalese and tech speak.

In terms of process, the team that creates a privacy policy should include all relevant Web site policy makers, legal advisors, the Webmaster, data managers, and others.

E. Privacy Audits

A privacy audit is designed to examine how an organization, such as a government agency, manages the personal information it collects. The goal is to determine whether such information is handled according to applicable privacy principles. An audit first determines what privacy laws and regulations the organization is subject to. Auditors then examine the organization's information processing procedures, including methods used to collect, store and distribute information about

⁷⁰ The Canadian government's "Guide to Writing a privacy Notice," http://www.cio-dpi.gc.ca/pgol-pged/nandc-aetc/nandc-aetc07_e.asp, includes examples of privacy notices http://www.cio-dpi.gc.ca/clf-upe/5/5ex2_e.asp.

individuals, to determine whether those procedures comply with relevant privacy requirements. The audit should identify any deficiencies that need to be corrected.

For example, in 1999, Australia's Office of Federal Privacy Commissioner ("OFPC") conducted a pilot audit of government websites to assess whether they complied with the country's information privacy principles.⁷¹ The OFPC conducted a more formal audit of compliance in 2000, and the results were presented to the various agencies. In May 2001, the OFPC initiated a follow-up audit of government websites to assess progress with compliance. The results of the third audit, which were published, indicated that almost one-third of Australia's government's agencies failed to meet the necessary requirements, such as displaying a privacy statement on the website.⁷² Thus, the audit helped bring pressure on the agencies to conform to applicable government privacy standards.

1. What are the elements of a privacy audit?

Although the specifics of audits will vary depending on the type of information system being evaluated, the major areas of inquiry for a privacy audit will often include the following:⁷³

- Collection processes
 - What data is collected?
 - Is it collected with or without the knowledge and consent of citizens?
 - For what purpose is each class of data being collected?
 - Specific questions in the Web context might include:
 - Are identifying data of visitors to government Web sites, such as IP addresses, automatically logged?
 - Are cookies used by government Web sites to track users?
- Retention
 - How long is data retained?
 - Are there procedures for deleting data after a certain time period?
- Use and disclosure
 - What uses are permitted for each class of data?

⁷¹ Privacy Compliance Audit: Commonwealth Government Web Sites 2001, August 2001, available at: <http://www.privacy.gov.au/publications/wsr01.html>.

⁷² See Media Release: Less Than 100% Compliance: Not Acceptable!, Office of the Privacy Commissioner, August 20, 2001, available at: http://www.privacy.gov.au/news/media/01_09_print.html.

⁷³ See, for example, The Privacy Audit: A Primer, by Pamela Jerskey, Ivy Dodge, Sanford Sherizen, available at <http://www2.bc.edu/~jerskey/privacy.htm>, and the privacy audit checklist posted at: <http://cyber.law.harvard.edu/clinical/privacyaudit.html>.

- To whom can the data be disclosed?
 - Are procedures in place to control the dissemination of personal data?
 - How is information being distributed within the organization?
 - Is personal information transferred to third parties or vendors?
 - How is data being used, protected and distributed after being transferred to third parties?
- Security
 - Is access to data held by government agencies restricted to authorized individuals?
 - What authentication, password and identification procedures are in place to prevent unauthorized employees from gaining access to data?
 - Does the agency protect the integrity and security of confidential data that is shared by multiple users?
 - Have policies been adopted and made known to all employees to control access to, and control of, shared confidential data?
 - Is confidential data properly marked as such?
 - Management
 - Who within the organization will implement and promote the policies and procedures governing privacy?
 - Does the organization's privacy policies define responsibilities of management and security administrators?
 - Who will oversee the organization's efforts to enforce these measures?

2. What are some of the most frequent deficiencies found during privacy audits?

Privacy audits frequently identify a significant gap between an organization's written privacy policies and its actual implementation of these policies. This suggests that the adoption of privacy policies and procedures is not sufficient. It is crucial that management and employees within the government also receive training on the meaning and operation of all privacy policies.

3. When should a privacy audit be performed?

Audits should be performed on a routine basis, before problems arise or abuses occur. Audits are increasingly being performed on a proactive basis to determine the potential flaws in an organization's privacy practices. There often are educational and organizational benefits to be gained from preemptive audits. In addition, however, audits may be initiated in response to complaints filed with a Privacy Commissioner, with the relevant agency head, or with the legislature.

IV. Emerging Issues

A. Public Records Online – the Court Records Example

Many details of an individual's life, activities, and personal characteristics can be found scattered throughout the files of government agencies. Many of these records are, by law or tradition, open to public inspection. This transparency serves important democratic values. But in the Internet Age it also poses privacy risks. It is now increasingly possible to construct a detailed profile of an individual using only publicly available, individually identifiable information from government records. While the types of government records that are publicly available vary from jurisdiction to jurisdiction, publicly accessible government records with personal information may include property ownership and tax records (name, address, value of property); driver's license (name, address, date of birth, physical characteristics, ID number); voter registration files; and occupational licenses. Information may also be publicly available about individuals who are required to file information on stock ownership with the stock exchange regulators; political candidates and government employees required to file ethics disclosure forms with state or federal offices; and recipients of government contract.⁷⁴

Court records in particular often contain a very large amount of personal information. There may be information available in public records about an individual who has interacted with the courts as a criminal defendant, as a plaintiff or defendant in civil litigation, as a juror, through divorce proceedings, in bankruptcy proceedings, as a beneficiary of a will, or in other ways.

The openness of judicial proceedings has always been a fundamental principle of the court system in the United States. In the US, for example, most court files have been open to anyone willing to come down to the courthouse and examine them. The reason that court files are open is to allow the public to monitor the functioning of the judiciary, to find out the status of cases and how they are resolved, in order to ensure fairness and impartiality through transparency.

However, the courts are finding themselves faced with some unexpected consequences of such an open access system as they become increasingly reliant upon the Internet. With caseloads growing each year, the Internet has become a valuable tool for court officials in terms of managing cases in an efficient and timely manner and streamlining document processing. At the same time, courts are using the Internet to give the public electronic access to court records, making judicial proceedings more transparent but also making widely available personally identifiable and sometimes

⁷⁴ Five Strategies for Addressing Public Register Privacy Problems, Blair Stewart. Assistant Commissioner, Office of the Privacy Commissioner, New Zealand <http://www.pco.org.hk/english/infocentre/files/stewart-paper.doc>. See also http://europa.eu.int/information_society/topics/telecoms/internet/public/index_en.htm

sensitive information that, while legally a matter of public record, used to be practically obscure.

As a result of technological innovations, more court records are in electronic form and thereby are more easily and widely accessible. Information in court records can now be made available through the Internet. Information in court records can be easily compiled in new ways. An entire database can be copied and distributed to others. These new circumstances require new access policies to address the concern that the proper balance is maintained between public access, personal privacy, and public safety, while maintaining the integrity of the judicial process.⁷⁵

In the US, the Conference of Chief Justices (CCJ) and the Conference of State Court Administrators (COSCA) developed guidelines on public access to provide guidance to judges and court administrators.⁷⁶ The *CCJ/COSCA Guidelines* are based on the following general principles:

- Retain the traditional policy that court records are presumptively open to public access.
- As a general rule, access should not change depending upon whether the court record is in paper or electronic form. Whether there should be access should be the same regardless of the form of the record, although the manner of access may vary.
- The nature of certain information in some court records, however, is such that remote public access to the information in electronic form may be inappropriate, even though public access at the courthouse is maintained;
- The nature of the information in some records is such that all public access to the information should be precluded, unless authorized by a judge;
- Access policies should be clear, consistently applied, and not subject to interpretation by individual court or clerk personnel.

⁷⁵ Beth Givens of the Privacy Rights Clearinghouse outlined recommendations on how to protect privacy in court records in a paper presented at the Computers, Freedom and Privacy Conference in 2002:

<http://www.cfp2002.org/proceedings/proceedings/givens.pdf>

⁷⁶ Martha Wade Steketee, Alan Carlson, *Developing CCJ/COSCA Guidelines for Public Access to Court Records: A National Project to Assist State Courts*, October 18, 2002 developed by the National Center for State Courts and the Justice Management Institute, on behalf of the Conference of Chief Justices and the Conference of State Court Administrators <http://www.courtaccess.org/modelpolicy/>. See also Administrative Office of the US Courts, Judicial Conference Committee on Court Administration and Case Management, *Report on Privacy and Public Access to Electronic Case Files*. Washington DC: US Courts, June 26, 2001.

http://www.uscourts.gov/Press_Releases/att81501.pdf.

The guidelines offer a very nuanced approach. For example, while the guidelines allow some information to be withheld from the public in order to protect privacy, they state that there shall be a publicly accessible indication of the existence of information in a court record to which access has been prohibited, which indication shall not disclose the nature of the information protected. In other words, if information is withheld from public access, it should be made apparent that something is being withheld. Making the existence of restricted information known enhances the accountability of the court. In addition to disclosing the existence of information that is not available, there is also a value in indicating how much information is being withheld. For many redactions this could be as simple as using “placeholders,” such as gray boxes on an electronic document, showing how much information has been excluded. Providing this level of detail about the information contributes to the transparency and credibility of the restriction process and rules. This is one way in which careful system design can effectively balance competing public policy interests.

If a court is considering making information in court records available electronically and remotely, for example on-line through a web site, they should consider whether some categories of information might, instead, only be accessible at a court facility within the jurisdiction.

The following categories of information might be withheld from public access or might be made available only at a court facility.

- Addresses, phone numbers and other contact information for victims (not including defendants) in domestic violence, stalking, sexual assault, and civil protection order proceedings;
- Addresses, phone numbers and other contact information for victims in criminal cases;
- Addresses, phone numbers and other contact information for witnesses (other than law enforcement witnesses) in criminal, domestic violence, sexual assault, stalking, and civil protection order cases;
- Social security numbers;
- Account numbers of specific assets, liabilities, accounts, credit cards, and PINs (Personal Identification Numbers);
- Photographs of involuntary nudity;
- Photographs of victims and witnesses involved in certain kinds of actions;
- Obscene photographs and other materials;
- Medical records;
- Family law proceedings including dissolution, child support, custody, visitation, adoption, domestic violence, and paternity, except final judgments and orders;
- Termination of parental rights proceedings;
- Names of minor children in certain types of actions.

In the US, the National Consortium for Justice Information and Statistics (SEARCH), in conjunction with the Department of Justice's Bureau of Justice Statistics

(BJS), has also examined the issue of privacy and electronic access to court records. In addition to issuing several studies on privacy and court records, SEARCH and BJS sponsored the National Task Force on Privacy, Technology and Criminal Justice Information <http://www.search.org/publications/pdffiles/Privacyproceed.pdf> and issued the Report of the National Task Force on Privacy, Technology, and Criminal Justice Information, August 2001 <http://www.ojp.usdoj.gov/bjs/abstract/rntfptcj.htm>.

In the US, the National Criminal Justice Association has issued an excellent guide on justice information systems: “Justice Information Privacy Guideline – Developing, Drafting and Assessing Privacy Policy for Justice Information Systems.” The goal of this *Guideline* is to provide assistance to government officials who seek to balance public safety, public access, and privacy when developing privacy policies for their agencies' systems, whether already operating or being planned and whether independent of or integrated with those of other agencies. The guideline addresses how the Fair Information Practices can be applied to criminal justice system information. It includes a set of “Privacy Design Principles” for justice information systems. It also addresses the various issues posed by public access.⁷⁷

B. Cybersecurity

A number of countries have gone through a series of steps in addressing the cyber-security issue: (1) study by a high-profile board, thereby conceptualizing and drawing attention to the problem; (2) Presidential designation of leadership within the executive branch to push the development of policy; (3) drafting of a national plan based on dialogue with all affected sectors; (4) adoption of legislation strengthening duties and authorities within the federal government.⁷⁸

Cyber-security is a process that establishes baselines of operations and inventories of systems, processes, technologies, networks, and software, identifies threats, vulnerabilities and risks, forms a strategy to weigh and manage the risks, implements the strategy, tests the implementation continuously, and monitors the environment to control the risks or improve upon protections. Security is not just about installing the latest security devices and deploying the most modern security technologies. Information security is a combination of business, management and technical measures on an ongoing

⁷⁷ <http://www.ncja.org/pdf/privacyguideline.pdf>. See also Daniel J. Solove, Access and Aggregation: Public Records, Privacy, and the Constitution, 86 Minnesota Law Review 6 (2002).

⁷⁸ See International Critical Information Infrastructure Protection Handbook, edited by Andreas Wenger, Jan Metzger and Myriam Dunn, Center for Security Studies and Conflict Research, Swiss Federal Institute of Technology (2002) <http://www.isn.ethz.ch/crn>.

basis. It is a process, not an end result. A cyber-security program⁷⁹ should include the following basic elements:

- Compile an inventory of the information assets of the organization.
- Ascertain what vulnerabilities and threats (internal and external) affect those assets.
- Assess the damage that would be caused to the institution if the vulnerabilities were successfully exploited by those threats.
- Determine what measures are appropriate to protect information assets.
- Implement risk management processes and security measures to safeguard the confidentiality, integrity and availability of computer-based assets, including, but not necessarily limited to –
 - Install firewalls, anti-virus software and intrusion detection systems;
 - Deploy strong cryptographic protection of sensitive data;
 - Develop and implement adequate policies;
 - Undertake constant training of personnel;
 - Maintain network surveillance and security monitoring;
 - Conduct testing;
 - Establish a incident response and recovery capability including back-ups and alternate site operations if appropriate.⁸⁰

There are various standards and best practices that are available to guide companies seeking to cope with their potential legal liability for cyber-security.

In January 2001, the Commission issued a Communication entitled *Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-Related Crime*⁸¹, in which it surveyed the problems cybercrime poses for national law enforcement authorities. The Communication also reviewed the

⁷⁹ The Computer Security Resource Center (CSRC) at the US government's National Institute of Standards and Technology (NIST) provides a public guide to creating information security policies. This technical guide to Internet security policies identifies various types of policies ranging from general direction setting policies to particular procedure/technology related policies to system-specific policies.

⁸⁰ Monetary Authority of Singapore, *Technology Risk Management Guidelines for Financial Institutions*, version as of 3 December 2002, at 3.

⁸¹ European Commission, *Communication from the Commission to the Council, the European Parliament, the Economic and Social Committee and the Committee of the Regions - Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime (COM(2000) 890 final, Brussels, 26.1.2001)*, online at:

<http://europa.eu.int/ISPO/eif/InternetPoliciesSite/Crime/CrimeComEN.pdf> (date accessed; 23 March 2003).

substantive and procedural laws in EU member states as they apply to cybercrime investigations and prosecutions. In light of its findings, the Commission made several recommendations, both legislative and non-legislative, aimed at improving security in cyberspace, including the harmonization of criminal prohibitions against hacking, denial of service attacks, and child pornography. The recommendations in the Communication also address procedural matters, such as increasing mutual recognition of pre-trial orders in order to facilitate cybercrime investigations.

In June 2001, the Commission issued a second Communication related to cyberspace security, entitled *Network and Information Security: Proposal for a European Policy Approach*.⁸² This Communication articulated a common European approach to policy development on network and information security issues, and proposed several initiatives, such as affirming support for the free circulation of encryption products and the further harmonization of national criminal laws relating to attacks against computer systems.

C. Authentication and Relationship Management

Authentication is a procedure used in the online environment to prove that a credential (such as a name, an IP address, or another identifier) is accurate, trustworthy, or genuine. Authentication can be anonymous, such that data cannot be associated with a particular individual, either from the data itself, or by combining the transaction with other data. Or authentication can be focused on identity -- an authentication process can be designed to make an association with a particular individual. Authentication can also be "pseudonymous," meaning that the process that cannot, in the normal course of events, be associated with a particular individual.

Interest in authentication systems has increased dramatically over the last two years, both in e-commerce applications and for e-government. The development of e-government services has begun to focus partly on plans to develop authentication systems to enhance citizen-centered government. However, ongoing discussions about government use of authentication systems raise concerns about government use of personal information and the creation of a centralized identity system or card. Widespread adoption of the technologies will only occur if individuals trust that strong privacy and security protections have been built into authentication systems.⁸³

⁸² European Commission, *Communication from the Commission to the Council, the European Parliament, the European Economic And Social Committee and the Committee of the Regions - Network and Information Security: Proposal for a European Policy Approach (6 June 2001)*, online at: http://europa.eu.int/information_society/eeurope/news_library/new_documents/index_en.htm (date accessed: 24 March 2003).

⁸³ See generally, *Authentication of Identity for E-Government*, Statement by Privacy Commissioner, Bruce Slane, 10 March 2003 <http://www.privacy.org.nz/media/e-govt.html>

New technologies for authentication make possible greater realization of the Internet's potential by making online transactions more seamless, tying together information on multiple devices, enabling yet unimagined services and taking us a few steps closer to a pervasive computing society. However, many authentication systems will collect and share personally identifiable information, creating privacy and security risks. To mitigate these risks, it is essential that authentication systems be designed to support fair information practices and offer individuals greater control over their personal information.

The Center for Democracy and Technology, through a consultative process involving a working group comprised of companies and public interest groups, has drafted basic privacy principles that should be considered in the design and implementation of authentication systems. These principles could be used by companies developing authentication systems for guidance in building privacy and security protections into authentication technologies to use in consumer initiated transactions and government services. The principles also serve as a guide for governments deciding which authentication system to implement or adopt. The principles are:

1) Provide User Control — *The informed consent of the individual should be obtained before information is used for enrollment, authentication and any subsequent uses.*

Consent controls are vital to building trust in authentication systems. Authentication systems should offer individuals meaningful control over disclosure of their information. Under this principle, individuals may choose to use a single form of authentication that always discloses the same information or credential for all interactions, or choose to employ a variety of authentication tools for different transactions. This principle is particularly important in data sharing and transfer systems, which will be successful only if they balance added convenience with trust in the system. Individuals should not be forced to accept the sharing of information for secondary uses as a condition of utilizing the authentication or data transfer system.

2) Support a Diversity of Services — *Individuals should have a choice of authentication tools and providers in the marketplace. While convenient authentication mechanisms should be available, privacy is put at risk if individuals are forced to use one single identifier for various purposes.*

Concerns persist that one or a very few implementations will be used for multiple purposes, coercing individuals and diminishing the ability of authentication systems to enhance privacy. This need not be the case. Authentication systems should be designed to support development of a marketplace offering multiple services that deliver varying degrees and kinds of authentication. A marketplace with a diversity of services also helps to support the principle of user control. Rather than attempt to serve as the perfect

single key, authentication services for individuals should function like keys on a key ring, allowing individuals to choose the appropriate key to satisfy a specific authentication need. Different government agencies, companies and organizations will likely need different types of authentication.

3) Use Identity Authentication Only When Appropriate —*Authentication systems should be designed to authorize individuals by use of identity when needed to complete the transaction. Identity need not and should not be a part of all forms of authentication.*

Not all transactions need be tied to identity. In fact, different kinds of authentication happen all of the time. For example, a store may need only to verify that an individual can pay for a service without collecting personal information, as we do today with cash transactions. Or, in another example, a membership organization may need to verify that an individual is authorized to partake in an activity without gaining access to detailed personal information. Different types of transactions require different levels of confirmation.

Authentication systems that use identity create greater privacy concerns as they can become ripe for abuse and targets for identity fraud and theft. Identity based authentication should only be used when necessary. Providing anonymous and pseudonymous authentication will be important to enabling user control, supporting a diversity of services and protecting privacy.

Identity credentials are particularly sensitive information. Secondary use and sharing of identity credentials for purposes such as marketing will compromise privacy and security. In particular, entities should be aware that Identification numbers become open to greater privacy misuses if they are often used for secondary purposes. Therefore, multiple uses of these numbers should be discouraged.

4) Provide Notice —*Individuals should be provided with a clear statement about the collection and use of information upon which to make informed decisions.*

Notice should be given in a manner consistent with the technology and be provided before information is used for enrollment, authentication and any subsequent use. Notice should not occur several links removed from the enrollment and authentication processes. The notice should in no way be a burden to read or understand.

5) Minimize Collection and Storage—*Institutions deploying or using authentication systems should collect and store only the information necessary to complete the intended authentication function.*

Authentication systems can collect and share information in several ways. They may collect sensitive information for enrollment, vetting and verification of an individual; they may use a subset of a user profile as the primary purpose of any intended authentication; and they may facilitate the onward transfer of information for secondary

purposes. It may be necessary to store some information to provide ongoing services. Information on retention practices should be available. In every instance, the information collected and stored should be limited to the minimum necessary to provide the intended authentication and service.

6) Provide Accountability - *Authentication providers should be able to verify that they are complying with applicable privacy practices.*

Privacy practices must be the cornerstone to building a trust relationship in authentication.⁸⁴ Training and regular audits are necessary to ensure that reasonable technical, administrative and physical privacy and security safeguards are in place. New privacy technologies can aid in tracking data flows for these purposes. Individuals, with appropriate authentication, should be able to access their own information used in the ordinary course of business and correct inaccurate information.

⁸⁴ All organizations collecting, maintaining or using personally identifiable information should develop internal practices that address applicable regulatory and self-regulatory guidelines, such as, the OECD Fair Information Practices Principles, the EU Directive on Data Protection.