

Submitted by the Department of Interior,
Office of Information Resources Management
Contact: Marilyn Legnini, Departmental Privacy Act Officer,
202-219-0868, Marilyn_Legnini@doi.gov

Challenges and Opportunities: Privacy
Information Privacy - A Key Element in E-Government

I. Changes in the Privacy Landscape

Developments in technology have resulted in the ability to communicate and obtain information electronically at unparalleled levels. The Information Age--e-government, e-services, e-commerce, e-benefits, e-mail--provides exceptional opportunities to communicate, do business, and share information. With the ever-increasing on-line and wireless/mobile capability, come new concerns. Information can be accumulated and combined to create powerful information packages on an individual or business that can be easily manipulated and combined with other information and sent instantly and globally, with no ability to retrieve the sent information or control its further dissemination.

A January Hart-Teeter Poll survey conducted on behalf of the Council for Excellence in Government indicates more than two to one Americans want to proceed slowly rather than quickly in implementing e-government because of concerns about security and privacy.¹ It is anticipated that more than 2.8 billion dollars were lost last year when the potential consumer's sense of privacy was offended and he/she terminated an on-line transaction.²

In this context, both private industry and the government must remain not only aware of the privacy concerns of their constituencies, but just as importantly, proactive in developing institutional safeguards which focus on developing strategy and policies for protecting personal information while increasing on-line services. In just the last few years there has been a great deal of discussion and opportunity to identify methodologies to achieve this goal. The importance is evident in new legislation, Administrative proclamations, and a flurry of guidelines on the need to address privacy in information systems and the Internet.

The challenge is taking advantage of the power of technology with efficient, effective, and accessible services, while at the same time safeguarding privacy and security and ensuring the confidence of its users.

II. What is Informational Privacy and Its Policy Framework?

Informational privacy -- the "right to be let alone"³ -- the right to control information about oneself and, conversely, the right to prevent nonconsensual access to information about oneself⁴

¹*E-Government: The Next American Revolution*, February 2001.

²*Forrester Research*, September 1999.

³*Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

⁴See Alan F. Westin, *Privacy and Freedom*, (Atheneum 1967), 7.

is not a new concept. An individual has the right to control the conditions under which information pertaining to him is collected, used, and disseminated.⁵

In 1974, Congress recognized a statutory right of privacy when it passed the Privacy Act (5 U.S.C.552a). The Act states that “the right to privacy is a personal and fundamental right protected by the Constitution of the United States.” The statute was an outgrowth of the Code of Fair Information Principles developed by the Department of Health, Education and Welfare (HEW) in 1973. The basic principles of the HEW Code are that there be no personal data record keeping systems whose existence is secret; there be a way for an individual to determine what information is in his or her file and how the information is being used; there be a way for an individual to correct such information; there be a way to assure the reliability of the data for its intended use and any organization creating, maintaining, using or disseminating records of personally identifiable information must take precautions to prevent misuse; and there 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.

The Privacy Act governs the use of information by federal agencies by restricting the disclosure of personally identifiable information without the individual's consent,⁶ granting an individual an increased right of access to agency records maintained on himself/herself,⁷ granting the individual the right to amend an agency record upon his demonstration that the record is not accurate, relevant, timely or complete,⁸ and establishing a code of fair information practices.⁹ Privacy legislation enacted by Congress supports the idea that there exists in certain circumstances a "reasonable expectation" of privacy.¹⁰

The existing legal framework identifies the degree of privacy a person may reasonably expect in cyberspace. Efforts to meet those expectations and developing standards to define the boundaries of privacy in cyberspace must be met through strategy and developing safeguards. Privacy also must be incorporated into the system development strategy and not stove-piped as it has been in the past.

The perception of privacy must change to that of a value added to a project and not a barrier to meet project goals. Tools to ensure that privacy is embedded in system and program requirements must be in place. Those explained below can be used to advance any organization's privacy protection goals.

⁵ See Privacy and the National Infrastructure: Principles for Providing and Using Personal Information, Privacy Working Group, Information Policy Committee, Information Infrastructure Task Force, 6 June 1995.

⁶ 5 U.S.C. § 552a(b).

⁷ 5 U.S.C. § 552a(d)(1).

⁸ 5 U.S.C. § 552a(d)(2).

⁹ 5 U.S.C. § 552a(e)

¹⁰ Other Congressional actions have addressed specific types of information maintained by the Executive Branch for which an individual has a “reasonable expectation” of privacy. See, e.g., The Electronic Communications Privacy Act of 1986, 18 U.S.C. §§ 1367, 2232, 2510-2511, 2701-2711, 3117, 3121-3127(restrictions for federal government access to records of electronic communications service providers); and The Children's Online Privacy Protection Act of 1998 (to ensure that web sites aimed at children will not gather personal information except with the consent of the parents).

III. A Privacy Program Strategy

A. The Privacy Program in the Organizational Structure:

The Department of Interior DOI like many corporate entities, began the conversion of its paper records into electronic data systems to improve business processes and enhance customer service. The Department of the Interior in recognizing the privacy concerns with increased systems reorganized its Privacy Act Program under the Chief Information Officer (CIO), Office of Information Resources Management (OIRM). This was consistent with the focus of information resources management presented in the Office of Management and Budget (OMB) Circular A-130: Management of Federal Information Resources revised in 1996 and 2000. The benefit of placing the Privacy Program under a CIO is evident of the privacy requirements identified in the Clinger-Cohen Act and OMB guidelines on the implementation of the Government Paperwork Elimination Act.

By aligning the Privacy Program under the CIO, it provides the program with more visibility organizationally. It promotes an environment that facilitates communication, coordination, and partnering with the other IT disciplines responsible for other aspects of information resources management. Privacy strategies have to be dynamic with the rapid changes in technology. This organizational structure helps to ensure that privacy specialists can keep up with the latest trends and analyze any potential privacy concerns. Privacy programs must be proactive and involved in order to keep pace with the issues.

B. Privacy Awareness:

The paradigm has changed. Where information in paper form was funneled through information specialists - the Information Collection Officer, Records Officer, Freedom of Information Act Officer, and Privacy Act Officer, etc. - when there was a question on how to handle information, other employees are now making decisions about information and data which would have been addressed through these specialists. For example, webmasters and program offices may have a primary goal to publish electronic information, or design pages to collect information off a web site without being aware of the different legal requirements. The Department tries to bridge this gap through training.

The Department considers Privacy Awareness an essential tool in ensuring that all employees making decisions on information are aware of their responsibilities in implementing statutory requirements and Administrative guidelines. OIRM's training strategy's focus is not only to update privacy specialists on recent developments in privacy, but to educate management and technology-related personnel. For example, Departmental Deputy Chief Information Officers, Webmasters, data administrators and E-Government teams were given training on what they need to know about privacy requirements for their special areas.

C. Privacy Assessments and Information Life Cycle Management:

Not only does the perception of privacy have to change from a barrier to a value, but how it is applied - break with tradition and use the front-end approach. The key here is that privacy is considered early on. This is a proactive approach, not a reactive approach, an assessment vs. audit approach, which requires reviewing data sensitivity and effects on the system in its developmental stages. Government initiatives in the last few years are stressing the focus on data when it is created and how it is used before systems are developed, and being able to identify vulnerabilities based on data sensitivity and data flow from the start.¹¹

This entails breaking the stove-pipe approach to collecting, maintaining, using, and safeguarding data, and coordinating with parties involved with the system and requiring a more strategic and integrated approach. Section 8a.(1)(a) of the OMB Circular A-130 requires that all agencies consider at each stage of the information life cycle, the effects of decisions and actions on other stages of the life cycle, particularly those concerning information. An information life cycle includes creation, maintenance and use, and disposition. Section 8a.(1)(j) requires that agencies “consider the effects of their actions on the privacy rights of individuals, and ensure that appropriate legal and technical safeguards are implemented.”¹²

The concept of applying privacy principles to the life cycle (cradle to grave) approach to information is important and applicable for government agencies and non-government organizations as they plan new systems or modify others.

1. Legal Admissibility of Records

In 1994 a checklist was developed by the Bureau of Land Management (BLM) called the “Official Agency Record Designation Document” (OARDD)(H-1270-1). The Bureau is responsible for maintaining millions of historic land patents and land use records. In its modernization initiative over the past decade and a half BLM increasingly converted paper records to electronic formats.

The documentation required in this directive lays the proper foundation or “...the requirement of introducing evidence of things necessary to make further evidence relevant, material, or competent” for admitting electronic records as evidence in court. The elements of the checklist include the following sections: (1) Administrative/statutory which address records, Freedom of Information Act, Privacy Act, and data sharing requirements; (2) Data integrity which covers

¹¹ The Presidential Decision Directive 63: Protecting America’s Critical Infrastructures calls for a national effort to assure the security of the U.S.’s increasingly vulnerable and interconnected infrastructures. Each agency is required to develop a plan for protecting its own critical infrastructure. Sensitive information must be identified, and threats to it addressed.

¹² OMB Circular A-130 provides uniform government-wide information resources management policies as required by the Paperwork Reduction Act of 1980, as amended by the Paperwork Reduction Act of 1995, 44 U.S.C. Chapter 35. The Circular specifically addresses information resources management that is “the process of managing information resources to accomplish agency missions. The term encompasses both information itself and the related resources, such as personnel, equipment, funds, and information technology.

audit trails, system security, data quality standards; (3) Software reliability; and (4) Hardware reliability.

The Government Paperwork Elimination Act implementation guidelines suggest similar controls and documentation. The OARDD will be a useful tool to ensure that privacy is considered in a new or amended information system or application, and also just as importantly, to ensure that data in a data base meet the legal standards of trustworthiness for legal admissibility in court and mission needs.

2. Privacy Impact Assessments

In February of 2000 the federal CIO Privacy Subcommittee recommended that the Internal Revenue Service's (IRS) Privacy Impact Assessment (PIA) which was developed in 1995 by IRS privacy specialists be used by all federal agencies.¹³ The PIA is a series of questions that walk the business owner and information systems partner through a list of questions that address privacy through the design stage and every subsequent stage of development of the automated system or application.

Questions fall under the following subheadings: (1) Data in the System (e.g., What are the sources of the information in the system?; and How will data be verified for accuracy?); (2) Access to the Data (e.g., Who will have access to the data in the system?; and What controls are in place to prevent the misuse of data by those having access); (3) Attributes of the Data (e.g., Is the use of the data both relevant and necessary to the purpose for which the system is being designed?; and How will the data be retrieved?); and (4) Maintenance and Administrative Controls (e.g. What are the retention periods of data in this system?).

In a recent article by Christopher J. Dorobek, "Think of Privacy Early and Often, CIO Council Tells Agency Buyers", Government Computer News, 19 June 2000, CIO Council Co-Chair of the Security, Privacy, and Critical Infrastructure Committee is quoted in support of the PIA. "If agencies apply 70 percent of the document, they will be ahead of the privacy game... The council's privacy committee wanted agencies to have a template they could use for their own systems as they attempt to bring privacy more into the forefront."

D. Imbedding Privacy in IT Planning and Analysis

The Interior Privacy Program's strategy in the next year is to find methods to ensure that privacy is considered in developing standards for enterprise architecture, identifying privacy criteria in security analysis, and developing a privacy requirement checklist to be used for webmasters as they consider development of an agency web site.

Although mentioned together in many guidelines, it is important to remember that security and privacy interface but are very distinct programs. Security encompasses the responsibility for protecting the information and data, and ensures that desired policies are carried out, through a combination of technological and administrative means and legal deterrence.

As with security, organizations need to identify a separate privacy thread throughout the stages

¹³ See letter from the CIO Council adopting the PIA as a "best practice". Go to: <http://www.cio.gov/docs/IRS.htm>.

of development for a system/application. The following are enterprise architecture milestones developed by Vince Curtin of the Internal Revenue Service's (IRS) Privacy Advocate's Office for the IRS Modernization Initiative who made these available for this paper.

(1) Conceptual: Have privacy concerns/issues been addressed surrounding the data being considered? Data is a very important aspect of privacy protection in regard to privacy assessments. There are many questions which have to be asked up front about the legal issues which affect the collection of the information, the legal protections around the data which may have an effect on the design of the system.

(2) Design specification: At stage two, privacy concerns dealing with the architecture become clearer. These would include the user population; more specific data elements, and additional data not considered earlier. The risks to the privacy of the data become clearer (e.g., is Privacy Act protected information, financial data, etc.).

(3) Data element designation: At this stage privacy can be discussed in more specific terms. More risks/concerns become more evident.

(4) Implementation/roll-out: In looking at interfaces, type of system, user population, privacy impacts are more evident as user requirements become more defined.

(5) Operational stages of the system/application: Previous issues can be addressed at this stage. This analysis will reflect the privacy concerns considered at each state of the Life Cycle, and whether the appropriate legal and technical safeguards have been implemented. Access to data should be provided only where needed and when needed. Adequate controls will be built into the systems, not just added on later, to ensure the integrity of data.

Does your architecture framework model address privacy? Are privacy measures part of the planning, design and implementation phases of your enterprise-wide systems, and system development strategy, thus ensuring the confidentiality, integrity, and availability of information and systems?

E. Websites - Guidelines, Statutes and Public Confidence

In his Directive on E-Commerce, President Clinton underlined the importance of using the Internet for government e-commerce initiatives, but also with precautions¹⁴. In May 1998 OMB issued a memorandum entitled "Top Privacy Principles for Federal Web Sites" which was the first of a number of guidelines issued by the Administration on applying privacy principles to federal web sites.

Public trust in how a government office manages the information collected from its web sites is needed in order for web sites to be used for the purposes for which they are designed.

¹⁴ Bill Clinton, Directive on E-Commerce, 17 December 1999. He stated that: "Moreover, as public awareness and Internet usage increase, the demand for online Government interaction and simplified, standardized ways to access Government information and services becomes increasingly important. At the same time, the public must have confidence that their online communications with the Government are secure and their privacy protected."

The Interior Webmaster and Privacy Act Officer have partnered in developing a privacy checklist which will be included with other web requirements in a style guide being coordinated by the Webmaster. The checklist identifies the Privacy Act, Children On-line Privacy Protection Act, inter-agency data sharing requirements, and OMB requirements that webmasters must address before a web site becomes active.

Interior Privacy and Freedom of Information Act (FOIA) specialists work closely with program offices and discuss plans made for the web page to identify any privacy or FOIA concerns, making suggestions to limit privacy concerns. These integrated teams are another means of “breaking out of the box” and ensuring that those developing a system/application consider all requirements regarding the posting and collection of information.

F. Partnerships and E-Business Initiatives

The same tools above to protect privacy and ensure reliability of data can be carried over into intra-governmental and inter-governmental partnerships. For example, with FirstGov inter-agency initiatives a privacy assessment of all projects will be needed. Since inter-agency information is involved, there will be more Privacy Act implementation considerations with data collections from these web sites used to develop customer service programs.

Agreements on standards to address fair information practices is an increased challenge when applying the existing policy framework beyond the bureau and agency. For example when some partnerships beyond the Executive Branch are developed for projects a common ground and balance must be found. The Federal Geographic Data Committee (FGDC) developed Privacy Principles that were adopted in April of 1998. The intent was to provide a guide of fair information practices that FGDC members are committed to follow in handling of geographic-spatial data.

The FGDC and the Urban and Regional Information Systems Association (URISA) are currently collaborating on a workshop to address the privacy issues that arise when various sectors are subject to different statutory and case law authority. The purpose of the workshop is to identify privacy concerns in geographic information in regard to collection of information, maintenance of it, new applications of the information, and publication or access to the information and (2) develop tools to ensure that privacy considerations will be accessed with different business processes.

IV. Conclusion

Privacy protections in the Information Age can not take place in a vacuum or be stove-piped and treated as a discrete topic as it has in the past. Privacy measures need to be integrated in strategic planning and become a natural part of that strategic plan as are other statutory counterparts. A commitment to this proactive approach is a way to earn the public trust to encourage interaction with E-Government initiatives.