



PRIVACY ACT OVERVIEW

The Basic Concepts of the Act

FOIA/Privacy Act Training

Approved by:

Samuel P. Jenkins, Director, Defense Privacy and
Civil Liberties Office

1901 South Bell Street, Suite 920

Arlington, VA 22202

Ph: 703-607-2943

Presentation Outline

- **History of the Privacy Act**
- **Overview of the Privacy Act**
 - Safeguards
 - Policy Objectives
 - Applicability
 - Definitions
- **Privacy Act Provisions**
 - Conditions of Disclosure
 - Accounting of Disclosures
 - Individual's Rights of Access and Amendment
 - Agency Requirements
 - Civil and Criminal Penalties
 - System of Record Exemptions
- **OMB's Statutory Responsibilities**
 - Privacy Act of 1974
 - Paperwork Reduction Act of 1995
 - E-Gov Act
- **Privacy Challenges**
 - Technology Changes
 - Reducing use of SSN
 - Access Control
 - ISE
 - CUI
 - Web 2.0
 - Identity Theft
 - Reauthorization
 - Contractors

History of the Privacy Act Intent

- The Privacy Act of 1974, Public Law 93-579, was created in response to concerns about how the use of computerized databases impacts individuals' privacy rights.
- The Act, which became effective **27 September 1975**, and has been called a code of fair information practices, attempts to strike a balance between the Government's right to maintain information on individuals and the individuals' right to have his or her privacy protected against unwarranted intrusions.

History of the Privacy Act

The HEW Report (1 of 3)

- In 1973, the Department of Health, Education and Welfare (HEW) issued a report entitled “Records, Computers and the Rights of Citizens”.
- The HEW report recommended Congress adopt a code of fair information practice for automated personal data systems.

History of the Privacy Act

The HEW Report (2 of 3)

- Code of fair information practice for automated personal data systems
 - **Collection limitation.** There must be no personal data record keeping systems whose very existence is secret.
 - **Disclosure.** There must be a way for an individual to find out what information about him is in a record and how it is used.
 - **Secondary usage.** There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.
 - **Record correction.** There must be a way for an individual to correct or amend a record of identifiable information about him.
 - **Security.** Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

History of the Privacy Act

The HEW Report (3 of 3)

- The HEW report required organizations keeping automated databases on individuals to
 - Enact safeguards to protect this data, and
 - Report to the public each year what databases they were keeping and what kinds of information they held.
- The HEW report also recommended that the SSN should only be used where it is absolutely necessary, and that no agency should require someone to give their SSN unless specifically mandated by Congress.

History of the Privacy Act Passage

- The Act was passed hurriedly in the final week of the Ninety-Third Congress.
- No conference committee was convened to reconcile differences in the bills passed by the House and Senate.
- Staffs of the respective committees prepared a final version of the bill that was ultimately enacted.

History of the Privacy Act

The PPSC Report (1 of 2)

- The Privacy Act established the U.S. Privacy Protection Study Commission (PPSC) to evaluate the statute and to issue a report containing recommendations for its improvement.
- The Commission issued its final report and ceased operation in 1977.

History of the Privacy Act

The PPSC Report (2 of 2)

- The 1977 PPSC report concluded that the Act
 - Did not result in the benefits Congress intended.
 - Contained language that was unclear.
 - Relied too heavily on the definition of a 'system of record' that was restricted to databases where information is retrieved by personal identifier.
 - Required the publication of notices in the Federal Register that were ineffective since public readership is very limited and the notices lack sufficient detail.

The Privacy Act of 1974 Safeguards

- Requires government agencies to show an individual any records kept on him or her
- Requires agencies to follow “fair information practices”
- Places restrictions on how agencies can share an individual’s data
- Allows individuals to sue the government for violations of the Act

The Privacy Act of 1974

Policy Objectives

- To restrict disclosure of personally identifiable records maintained by agencies.
- To grant individuals increased rights of access to agency records maintained on themselves.
- To grant individuals the right to seek amendment of agency records maintained on themselves upon a showing that the records are not accurate, relevant, timely, or complete.
- To establish a code of "fair information practices" which requires agencies to comply with statutory norms for collection, maintenance, and dissemination of records.

The Privacy Act of 1974

Applicability

- U.S. citizens and aliens admitted for permanent residence.
- Executive departments, military departments, independent regulatory agencies, and government-controlled corporations
- Systems of records, i.e., any group of records where information is retrieved by the name of the individual or by an individual identifier.

Definitions (1 of 9)

- **Personally Identifiable Information.**
Information which can be used to identify a person uniquely and reliably, including but not limited to name, date of birth, social security number, address, telephone number, e-mail address, mother's maiden name, etc.

Definitions (2 of 9)

- **Agency.** An agency that promulgates rules in accordance with notice and comment rulemaking.

Definitions (3 of 9)

- **Individual.** A citizen of the United States or an alien lawfully admitted for permanent residence.

Definitions (4 of 9)

- **Maintain.** Includes maintain, collect, use or disseminate.

Definitions (5 of 9)

- **Record.** Any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual , such as a finger or voice print or photograph.

Definitions (6 of 9)

- **System of Records.** A group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual. **5 U.S.C. § 552a(a)(5).**

Definitions (7 of 9)

- **Routine Use.** With respect to the disclosure of a record, the use of each record for a purpose which is compatible with the purpose for which it was collected. 5 U.S.C. **§552a (a)(7)**

Definitions (8 of 9)

- **Matching Program.** Any computerized comparison of
 - Two or more automated systems of records with non-Federal records for the purpose of
 - Establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by applicants for, recipients or beneficiaries of, participants in, or provider of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or
 - Recouping payments or delinquent debts under such Federal benefit programs, or
 - Two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records

Definitions (9 of 9)

- **Federal Benefit Program.** Any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals.

Exceptions to the *No Disclosure to Third Parties Without Consent Rule*

1. **Need To Know**
2. **Disclosure Required By The Freedom Of Information Act (FOIA)**
3. **Routine Use**
4. **Disclosure To Census**
5. **Disclosure To An Individual Who Has Provided Adequate Written Assurance That The Record Will Be Used Solely For Statistical Research**
6. **Disclosure To The National Archives And Records Administration**
7. **Disclosure To Another Agency For Civil Or Criminal Law Enforcement Activity**
8. **Disclosure Under Emergency Circumstances**
9. **Disclosure To Either House Of Congress**
10. **Disclosure To The General Accounting Office**
11. **Disclosure Mandated By Court Order Of Competent Jurisdiction**
12. **Disclosure To A Consumer Reporting Agency In Accordance With The Debt Collection Act**

Consent

Defined as:

1. To permit, approve, or agree; comply or yield.
2. Permission, approval, or agreement; compliance; acquiescence.
3. Agreement in sentiment, opinion, a course of action, etc.

Conditions of Disclosure (1 of 15)

- **General Disclosure Prohibition:**
 - “No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains.”

Conditions of Disclosure (2 of 15)

- **“Need to Know” Within Agency**
 - This exception permits disclosure absent consent of the individual who is the subject of the record for:
 - The disclosure to officers and employees of the agency which maintains the record who have a need to know in the performance of their duties. 552a(b)(1)

Conditions of Disclosure

(3 of 15)

- **Disclosures made under the Freedom of Information Act.**
 - **If information must be released under FOIA, it must also be released under the Privacy Act.**
 - **No discretionary disclosures are allowed. Discretionary FOIA releases may not be made without an individual's consent, unless there is another applicable exception, such as "routine use."**
 - **Information that is protected under the Privacy Act is generally protected under FOIA. FOIA cannot be used to deny an individual information about him/herself.**
 - **The agency must be in receipt of an actual FOIA request for the information.**
 - **Only information that is not subject to a FOIA exemption (usually (b)(6) or (b)(7)(C)) will be required to be released.**

Conditions of Disclosure (4 of 15)

- **Disclosure for a “Routine Use.”**
 - Disclosure is authorized pursuant to routine use published in the Federal Register, compatible with the purpose for which it is collected. Routine use must be published in the Federal Register and include categories of users and the purpose of the use and must be compatible with the purpose for which the information was collected.
 - Agencies may always disclose records indicating a possible violation of law to law enforcement agencies for investigation/prosecution, regardless of the purpose for collection.
 - Agencies cannot include responses to subpoenas as routine use, since there is an exception for court orders which has been interpreted to exclude subpoenas.

Conditions of Disclosure

(5 of 15)

- **The disclosure is to the Census Bureau for the purposes of a census survey.**
 - Information may be disclosed to the Census Bureau in individually identifiable form for use by the Census Bureau pursuant to Title 13, which prohibits disclosure by Census.

Conditions of Disclosure

(6 of 15)

- **The disclosure is to someone who has adequately notified the agency in advance that the record is to be used for statistical research or reporting, and the record is transferred without individually identifying data.**
 - The record must be transmitted in a form that is not individually identifiable. A statistical record is one which is not used in making individual determinations.

Conditions of Disclosure (7 of 15)

- **Disclosure for Statistical Research and Reporting (1 of 2)**
 - **Subsection (b) (5)** “To a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable”
 - The use of the phrase “in a form’ that is not individually identifiable means not only that the information disclosed or transferred must be stripped of individual identifiers but also that the identity of the individual can not be reasonably deduced by anyone from tabulations or other presentations of the information (i.e., the identity of the individual can not be determined or deduced by combining various statistical records or

Conditions of Disclosure (8 of 15)

- **Disclosure for Statistical Research and Reporting (2 of 2)**
 - By reference to public records or other available sources of information.) See also the discussion of statistical record.
 - Fundamentally agencies disclosing records under this provision are required to assure that information disclosed for use as a statistical research or reporting record cannot reasonably be used in any way to make determinations about individuals.

Conditions of Disclosure

(9 of 15)

- **Disclosure To Another Agency Or To Any Governmental Entity Within Or Under The Control Of The United States For A Civil Or Criminal Law Enforcement Activity**
 - The law enforcement activity must be authorized by law.
 - The agency head must submit a written request to the agency that maintains the record.
 - The request must specify the particular portion of the record desired and the specific law enforcement activity for which the record is sought.
 - Records may be disclosed to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United State Government for a civil or criminal law enforcement activity if the activity is authorized by law and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the specific law enforcement activity.

Conditions of Disclosure (10 of 15)

- **Disclosure to the National Archives and Records Administration (NARA)**
 - Records can be disclosed if the record has sufficient historical or other value to warrant its continued preservation by the Government, or
 - For evaluation by the Archivist to make that determination.
 - Records which are transferred to the Federal Records Center for safekeeping do not fall within this category- they are not disclosures under the Privacy Act.

Conditions of Disclosure

(11 of 15)

- **Disclosure to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual.**
 - Disclosure may be made pursuant to a showing of compelling circumstances affecting the health or safety of any individual if upon such disclosure, notification is transmitted to the last known address of the individual.
 - This provision permits disclosure when, for example, the time required to obtain the consent of the individual to whom the record pertains might result in a delay which could impair the health or safety of any individual, as in the release of medical records to a person undergoing emergency medical treatment.
 - The individual to whom the records pertain need not be the individual whose health or safety is in peril.

Conditions of Disclosure (12 of 15)

- **Disclosure to Either House of Congress.**

(Includes any committee, subcommittee, or joint committee)

- Records may be disclosed to either House of Congress or, to the extent of matter within its jurisdiction, any committee or subcommittee, any joint committee of Congress, or subcommittee of any such joint committee. This does not authorize disclosure to members of Congress acting in their individual capacities, without the consent of the individual.
- The matter in question must be within its jurisdiction.

Conditions of Disclosure

(13 of 15)

- **The disclosure is made to the Comptroller General in the course of the duties of the General Accounting Office.**
 - Records may be disclosed to the General Accounting Office, to the Comptroller General, or any of his/her authorized representatives, in the course of the performance of duties of the GAO. Disclosure to the Comptroller General in the course of the performance of the duties of the Government Accountability Office (formerly Government Accounting Office).

Conditions of Disclosure

(14 of 15)

- **Disclosure Mandated By Court Order Of Competent Jurisdiction**
 - A subpoena does NOT qualify under this exemption unless it is specifically approved and signed by a Judge of a Court of competent jurisdiction.
 - A court of competent jurisdiction exists where an agency is a proper party in a federal case, the court's personal jurisdiction over the agency presumably exists and thus court ordered discovery of the agency's records is clearly proper.

Conditions of Disclosure (15 of 15)

- **Disclosure to a consumer reporting agency in accordance with the Debt Collection Act.**
 - Records may be disclosed to a consumer reporting agency in accordance with the Debt Collection Act. There are administrative steps that must be followed in connection with this section.

Accounting of Disclosures (1 of 2)

- An agency must keep accurate accounts of when and to whom it has disclosed personal records, including
 - Name and address of the person or agency to whom the disclosure is made, and
 - Date, nature and purpose of each disclosure.
- An accounting is not required for intra-agency (need-to-know) or FOIA disclosures.
- The accounting of disclosures must be kept for five years or the life of the record, whichever is longer.

Accounting of Disclosures (2 of 2)

- Unless the records were shared for law enforcement purposes, the accounts of the disclosure should be available to the data subject upon request.
- If an agency makes corrections or notations of dispute to any record, the agency must inform any person or agency to whom it has disclosed the original information, if an accounting of disclosures was made.

Individual's Right of Access (1 of 2)

- The Privacy Act permits only an "individual" to seek access to only his own "record," and only if that record is maintained by the agency within a "system of records"
- Upon request an individual may allow a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Individual's Right of Access (2 of 2)

- An individual's access request for his own record maintained in a system of records should be processed under both the Privacy Act and the FOIA, regardless of the statute(s) cited in the request.
- The accounting of disclosures must be kept for five years or the life of the record, whichever is longer.
- Unless the records were shared for law enforcement purposes, the accounts of the disclosure should be available to the data subject upon request.

Individual's Right of Amendment (1 of 2)

- An individual has the right to request amendment to his record.
- The agency must acknowledge receipt in writing, and promptly, i.e., within 10 working days of receipt of the amendment request
 - Make the requested correction, or
 - Inform the individual of refusal of the request and provide a reason for the refusal, the agency's procedure for a review of the refusal by the head of the agency and the name and business address of that official

Individual's Right of Amendment (2 of 2)

- The agency must permit an individual who disagrees with its refusal to amend his record to request review of such refusal, and not later than 30 working days from the date the individual requests such review, the agency must complete it.
- If the reviewing official also refuses to make the amendment, the individual must be permitted to file with the agency a concise statement setting forth the reasons for disagreement with the agency. The individual's statement of disagreement must be included with any subsequent disclosure of the record.

Agency Requirements (1 of 10)

- Maintain only information about an individual that is relevant and necessary to accomplish a legal purpose of the agency.
- Collect information to the greatest extent practicable directly from the subject individual if that information may have an adverse effect upon that individual.

Agency Requirements

(2 of 10)

- When collecting information from the individual, include the following on the collection form or on a separate form that can be retained by the individual (popularly referred to as the Privacy Act Statement)
 - The authority which authorizes the solicitation of the information
 - Whether disclosure of such information is mandatory or voluntary
 - The principal purpose or purposes for which the information is intended to be used
 - The routine uses which may be made of the information, and
 - The effects on the individual, if any, of not providing all or any part of the requested information.

Agency Requirements (3 of 10)

- Publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records. The system of records notice shall include
 1. The name and location of the system
 2. The categories of individuals on whom records are maintained in the system
 3. The categories of records maintained in the system
 4. Each routine use of the records contained in the system, including the categories of users and the purpose of such use
 5. The policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records

Agency Requirements (4 of 10)

6. The title and business address of the agency official who is responsible for the system of records
7. The agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him
8. The agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its contents; and
9. The categories of sources of records in the system.

Agency Requirements (5 of 10)

- Maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.
- Except in the case of FOIA releases, make reasonable efforts to assure that records are accurate, complete, timely, and relevant for agency purposes prior to disseminating any record about an individual to any person other than an agency.

Agency Requirements (6 of 10)

- Maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity.
- Make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.

Agency Requirements (7 of 10)

- Establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.
- Establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

Agency Requirements (8 of 10)

- At least 30 days prior to publication of information under a routine use(s) from a system of records, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.

Agency Requirements (9 of 10)

- An agency that maintains a system of records "shall promulgate rules, in accordance with notice and comment rulemaking."
 1. Establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him.
 2. Define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual.
 3. Establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedures, if deemed necessary, for the disclosure to an individual of medical records, including psychological records pertaining to him.

Agency Requirements (10 of 10)

4. Establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under the Act.
5. Establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.

Penalties for Non-compliance

- **Civil Remedies**

- The cost of actual damages suffered (\$1000 minimum)
- Costs and reasonable attorney's fees.

- **Criminal Penalties**

- Charge of a misdemeanor
- Maximum fine of \$5,000

Systems of Records Exempted from the Access Provisions of the Privacy Act

- An Agency may exempt a system of records from specified exemptions of the Act, all having to do with how an individual gets information about his records including:
 - Accounting to the individual (c)(3),
 - Accuracy of records (d), (e)(1),
 - Advising individual of existence of record pertaining to him or her (e)(4)(G),
 - Advising individual of how to gain access/amendment (e)(4)(H),
 - Sources of records, (e)(4)(I) and
 - Agency rules (f)

Systems of Records Exempted from the Access Provisions of the Privacy Act (1 of 10)

- **Exemption (d)(5):**
 - Information compiled in reasonable anticipation of civil action or proceeding; self-executing exemption

Systems of Records Exempted from the Access Provisions of the Privacy Act (2 of 10)

- **Exemption (j)(1):**
 - Records maintained by the Central Intelligence Agency

Systems of Records Exempted from the Access Provisions of the Privacy Act (3 of 10)

- **Exemption (j)(2):**
 - Records maintained by an agency which performs as its principal function any activity pertaining to the enforcement of criminal laws

Systems of Records Exempted from the Access Provisions of the Privacy Act (4 of 10)

- **Exemption (k)(1):**
 - Classified information under an Executive Order in the interest of national defense or foreign policy.

Systems of Records Exempted from the Access Provisions of the Privacy Act (5 of 10)

- **Exemption (k)(2):**

- Non-criminal law enforcement records; criminal law enforcement records compiled by non-principal function criminal law enforcement agency; coverage is less broad where individual has been denied a right, privilege, or benefit as result of information sought.

Systems of Records Exempted from the Access Provisions of the Privacy Act (6 of 10)

- **Exemption (k)(3):**
 - Pertain to the provision of protective services to the President of the United States or other individual pursuant to section 3056 of Title 18.

Systems of Records Exempted from the Access Provisions of the Privacy Act (7 of 10)

- **Exemption (k)(4):**
 - Required by statute to be maintained and used solely as statistical records.

Systems of Records Exempted from the Access Provisions of the Privacy Act (8 of 10)

- **Exemption (k)(5):**
 - Investigatory material used only to determine suitability, eligibility, or qualifications for federal civilian employment or access to classified information when the material comes from confidential sources.

Systems of Records Exempted from the Access Provisions of the Privacy Act (9 of 10)

- **Exemption (k)(6):**
 - Testing or examination material used to determine appointment or promotion of federal employees when disclosure would compromise the objectivity or fairness of the process.

Systems of Records Exempted from the Access Provisions of the Privacy Act (10 of 10)

- **Exemption (k)(7):**
 - Evaluation material used to identify potential for promotion in the Armed Services but only to the extent disclosure would reveal a confidential source who provided the info under an express promise of confidentiality.

Reduction of the Use of Social Security Numbers required by OMB Memo M-07-16

- **Eliminate Unnecessary Use.** Agencies must now also review their use of social security numbers in agency systems and programs to identify instances in which collection or use of the social security number is superfluous. Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of social security numbers within eighteen months.²²
- **Explore Alternatives.** Agencies must participate in government-wide efforts to explore alternatives to agency use of Social Security Numbers as a personal identifier for both Federal employees and in Federal programs (e.g., surveys, data calls, etc.).

Disclosure of the Social Security Number

- **It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual's refusal to disclose his social security account number.**
- **Any Federal, State or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.**

Privacy Act Implementation Challenges

- Technology changes
- The Internet
- Easily portable mass storage (thumb drives, laptops, CDs)
- Faster and faster computer processing speeds
- Increased interconnectivity of computer systems
- Practically everyone has a computer
- Areas of Act difficult to interpret and apply in today's environment
- Definitions - What is personal information...personally identifiable information ... PA protected information? How do we wrap our arms around it?
- Is there any system that does not retrieve by a personal identifier? Are we just engaging in wordplay?
- Is there pervasive abuse of 'routine uses'?

Privacy Act Implementation Challenges

- The Act gives the Director of the Office of Management and Budget the power to develop regulations and guidelines on how agencies should implement the Act.
- The Act is 35 years old. Can it still effectively regulate the collection, maintenance, use, and dissemination of personal information by today's federal executive branch agencies?
 - Technology has progressed exponentially since 1975
 - Some areas of the Act are difficult to interpret and implement
 - What's so 'routine' about routine uses? What are 'compatible' purposes?

Privacy Act Implementation Challenges

The U.S. Privacy Protection Study Commission (1977)

- Did not result in the benefits Congress intended.
- Contained language that was unclear.
- Relied too heavily on the definition of a 'system of record' that was restricted to databases where information is retrieved by personal identifier.
- Required the publication of notices in the Federal Register that were ineffective since public readership is very limited and the notices lack sufficient detail.

Privacy Act Implementation Challenges

- **The 2008 GAO Report Made Three Primary Findings**
 - The GAO found that the definition of a “system of records” is not universally applicable to the types of personally identifiable information collected by the government. The GAO recommended revising this definition to cover all personally identifiable information that is collected by the federal government.
 - The GAO found that the current privacy regime does not adequately control collection and use of personally identifiable information. In response, the GAO recommended that the law be amended to require agencies to justify collection of information and to justify the use or sharing of personally identifiable information.
 - The GAO found that current methods used to inform the public about policies and practices around government collections of information are ineffective. Specifically, Privacy Act notices are hard to understand and difficult to find. The GAO recommended the use of layered notices, in which the most important facts are presented to the user to begin with, followed by denser and more esoteric information as the user digs deeper. The GAO also recommended publishing these sorts of notices at a central, easy to access location on the Web.

Privacy Act Implementation Challenges

The Information Security and Privacy Advisory Board found that:

The Privacy Act and related policy should be brought up to date.

- **Amendments to the Privacy Act of 1974 and Section 208 of the E-Government Act of 2002 are needed to:**

- o Improve Government privacy notices;
- o Update the definition of System of Records to cover relational and distributed systems based on government use, not holding, of records.
- o Clearly cover commercial data sources under both the Privacy Act and the E-Government Act.

- **Government leadership on privacy must be improved.**

- o OMB should hire a full-time Chief Privacy Officer with resources.
- o Privacy Act Guidance from OMB must be regularly updated.
- o Chief Privacy Officers should be hired at all “CFO agencies.”
- o A Chief Privacy Officers’ Council should be developed.

- **Other changes in privacy policy are necessary.**

- o OMB should update the federal government’s cookie policy.
- o OMB should issue privacy guidance on agency use of location information.
- o OMB should work with US CERT to create interagency information on data loss across the government
- o There should be public reporting on use of Social Security Numbers

Privacy Act Implementation Challenges

- **Installation Physical Access Control Systems (1 of 2)**
 - Is PII being collected? If yes, under what SORN?
 - Where is PII being stored? Are your contractors storing the data?
 - Is the 'yes/no' decision for entry being kept in a database?

Privacy Act Implementation Challenges

- **Installation Physical Access Control Systems (2 of 2)**
 - How is the individual advised if a decision to deny entry is determined?
 - What sources of information are being used in the access decision? Is it a government authorized source that is reliable, timely and accurate?

Privacy Act Implementation Challenges

- **Social Security Number Use Reduction (1 of 2)**
 - DoD Directive-Type Memorandum 07-015-USD(P&R) “DoD Social Security Number Reduction Plan”
 - At every juncture, question why we’re collecting the SSN
 - Review use of SSNs and justifications

Privacy Act Implementation Challenges

- **Social Security Number Use Reduction (2 of 2)**
 - Review existing and new forms
 - Submit annual report with FISMA report
 - Crosscheck system inventories and systems of records notices

Privacy Act Implementation Challenges

- **Information Sharing Environment (ISE) (1 of 2)**
 - Composed of Five Communities
 - Intelligence
 - Law Enforcement
 - Defense
 - Homeland Security
 - Foreign Affairs

Privacy Act Implementation Challenges

- **Information Sharing Environment (ISE) (2 of 2)**
 - **Mission**
 - to share terrorism-related information through trusted partnerships so those who have information can share it and those who need information receive it,
 - in order to improve information sharing among federal entities; state, local, and tribal entities; the private sector; and our foreign partners.
 - The Privacy framework establishes core privacy protections and enables information sharing while ensuring appropriate safeguards for privacy and civil liberties protection for Americans citizens.
 - More information to follow

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (1 of 6)**
 - May 9, 2008 Presidential Memorandum mandates implementation of CUI framework within Information Sharing Environment (<http://georgewbush-whitehouse.archives.gov/news/releases/2008/05/20080509-6.html>)
 - “All departments and agencies shall apply the CUI Framework, ... for the designation, marking, safeguarding, and dissemination of any CUI terrorism-related information within the ISE that originates in departments and agencies, regardless of the medium used for its display, storage, or transmittal.”

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (2 of 6)**
 - NARA has been designated as the Executive Agent to implement the CUI framework (<http://www.archives.gov/cui/about/cuio.html>)
 - Three CUI designations replace “Sensitive But Unclassified (SBU)”

Privacy Act Implementation Challenges

- **CUI Designations (3 of 6)**
 - "Controlled with Standard Dissemination" meaning the information requires standard safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Dissemination is permitted to the extent that it is reasonably believed that it would further the execution of a lawful or official purpose.

Privacy Act Implementation Challenges

- **CUI Designations (4 of 6)**
 - "Controlled with Specified Dissemination" meaning the information requires safeguarding measures that reduce the risks of unauthorized or inadvertent disclosure. Material contains additional instructions on what dissemination is permitted.

Privacy Act Implementation Challenges

- **CUI Designations (5 of 6)**
 - "Controlled Enhanced with Specified Dissemination" meaning the information requires safeguarding measures more stringent than those normally required since the inadvertent or unauthorized disclosure would create risk of substantial harm. Material contains additional instructions on what dissemination is permitted.

Privacy Act Implementation Challenges

- **Controlled Unclassified Information (CUI) (6 of 6)**
 - The DoD has expanded the implementation of CUI to include all DoD CUI not just information that falls within the ISE.
 - OSD memorandum, “White House Approval of CUI Policy Framework”, July 21, 2008
 - USD(I) memorandum, “Clarification of Current DoD Policy on CUI”, April 7, 2009

Privacy Act Implementation Challenges

- **Web 2.0**

"Web 2.0 is fundamentally social, treating the individual at the center of the universe as opposed to groups or organizations, and then basing communication and information paths on social relationships between individuals."

- Stowe Boyd, DoD Web 2.0 Guidance Forum



Privacy Act Implementation Challenges

- **Web 2.0 Concerns**

- Favorite target of hackers
- Posting inappropriate content
 - Offensive language
 - PII (posting own or someone else's)
 - National security
- Personnel must ensure information posted to official social networking site is approved for public use
- Continuous monitoring is imperative

Privacy Act Implementation Challenges

- **Identity Theft**

- Constant threat to our organization
- Enforce awareness among personnel
- Report all breaches to DPO
- Conduct risk analysis to determine next steps in individual notification
- FTC Identity Theft Site
<http://www.ftc.gov/bcp/edu/microsites/idtheft/>

Privacy Act Implementation Challenges

- **Contractor Oversight (1 of 2)**
 - When an agency provides by contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of Section (m) to apply to such system, and
 - Any such contractor and any employee of such contractor shall be considered to be employees of an agency.

Privacy Act Implementation Challenges

- **Contractor Oversight (2 of 2)**

- FAR 52.224-1 Privacy Act Notification

http://www.defenselink.mil/privacy/files/sites_of_interest/FAR_52_224_1.pdf

- FAR 52.224-2 Privacy Act

http://www.defenselink.mil/privacy/files/sites_of_interest/FAR_52_224_2.pdf

- DFAR Part 224 - Protection of Privacy and Freedom of Information

<http://farsite.hill.af.mil/reghtml/regs/far2afmcfars/fardfars/dfars/dfars224.htm>

OMB's Statutory Responsibilities Privacy Act of 1974

- **The Privacy Act states that “The director of the Office of Management and Budget shall...provide continuing assistance to and oversight of the implementation of this section by agencies.”**
- **Guidance, Memos, consultation with agencies regarding Privacy Act inquiries**
- **Requires agencies to provide OMB with advance notice of new or significant changes to systems of records and matching programs.**
- **1975 Guidelines and Responsibilities/Circular A-130**
- **Comment on proposed legislation amending or affecting implementation of the Privacy Act.**

OMB's Statutory Responsibilities Paperwork Reduction Act

- **The Privacy Act states that “With respect to privacy and security, the Director (of OMB) shall...develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies...”**
- **It also requires OMB approval for collections of information from the public and provides opportunity for the public to comment on proposed information collections.**

OMB's Statutory Responsibilities E-Gov Act of 2002

- **The Privacy Act states that “With respect to privacy and security, the Director (of OMB) shall...develop and oversee the implementation of policies, principles, standards, and guidelines on privacy, confidentiality, security, disclosure and sharing of information collected or maintained by or for agencies...”**
- **It also requires OMB approval for collections of information from the public and provides opportunity for the public to comment on proposed information collections.**

Resources

- Privacy Act of 1974
- Federal Register July 9, 1975 Privacy Act Implementation-Guidelines and Responsibilities
- DOJ Overview of the Privacy Act of 1974, 2004 edition
- OMB Circular A-130
- Various OMB Memoranda
- Section 208 – E-Gov Act
- Federal Acquisition Regulations

Questions?

