Privacy Roots: SORNs and PIAs

Systems of Records Notices
TIMOTHY H. GRAHAM
U.S. DEPARTMENT OF VETERANS AFFAIRS
VETERANS HEALTH ADMINISTRATION

Policy Objectives of the Privacy Act
• To restrict disclosure of personally identifiable records maintained by the agencies
• To grant individuals an increased right of access and a right of amendment of records
• To establish a “code of fair information practices” that regulates the collection, maintenance, use and disclosure of personally identifiable records
• To grant individuals private rights of action for agency violations of the Act
Defining a Privacy Act “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 a photograph.

System of Records
- A group of any records, under the control of an 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.

Retrievability
- The standard under the Privacy Act is actual retrieval.
- OMB Guidelines outline what is actual retrieval:
  - A system of records exists if:
    - There is an indexing or retrieval capability using identifying particulars built into
      the system AND
    - the agency does, in fact, retrieve records about individuals by reference to some
      personal identifier.
System of Records Notice Requirements

- Must publish a system of records notice (SORN) in the Federal Register (5 U.S.C. § 552a(e)(4))

Types of SORNs

- SORNs may be agency wide, department wide or government wide.
- Typically, agencies publish SORNs in the Federal Register AND the agency’s website.
- SORNs should be in place before data collection.

Why are SORN's important?

- It’s the foundation of our Privacy programs. It helps identify the records that we collect and maintain.
- It’s transparency – enabling people to know what kinds of information we are collecting and on whom.
- It’s rulemaking
- It’s a blueprint that describes our business practice of collecting records.
- It’s the authority for sharing information with others.
- It’s something that we update regularly to reflect changes in business practices and ensure individuals understand how we use their personal information.
SORN Sections

• **System Location**: Identifies where the records are located – includes activity name and full address – should indicate where decentralized records are held.

• **Categories of Individuals Covered by the System**: Identifies who we are collecting information on (i.e., civilian employees, military members, contractor employees, dependents).

• **Categories of Records in the System**: Defines the kinds of records the Agency is maintaining, such as “Personal information that includes name, address, etc.”

SORN Sections (cont.)

• **Authority**: Identifies the basis for collecting the information (i.e., specific statute, regulation, executive order).

• **Purpose**: Addresses why you are collecting the information (i.e., To evaluate…; to nominate…; etc) and identifies any internal agency sharing of the information and for what purpose.

• **Routine Uses of Records maintained in the system, including categories of users and the purposes of such uses**: Identifies who outside the agency you can share the information with and for what purpose.

  - These are discretionary; Routine Uses do not REQUIRE sharing.
  - Usually require a written request, written response, and a disclosure accounting record.

SORN Sections (cont.)

• **Storage**: Should identify how is the information stored? Electronic database? Paper records? Microfiche?

• **Retrievability**: This is what makes it a PA system of records – must be retrieved by a name and/or personal identifier.

• **Safeguards**: Now that you have collected the information – this discusses how you will protect the information from unauthorized access.

• **Retention and Disposal**: Describes how long the records will be kept and how they will be disposed of (i.e., records are maintained for 6 years and then shredded; permanent – retired to NARA after 75 years).
SORN Sections (cont.)

• **System manager and address:** Identifies the responsible official for the system. This may be a specific office that is responsible for the system. Oftentimes, this is a high level policy official responsible for records.

• **Notification Procedure:** Describes who you should contact and what you should provide to determine if records are held on you.

• **Record Access Procedure:** Tells you who to write to and what to provide to identify yourself so records can be made available to you.

**QUESTIONS?**

SORN Sections (cont.)

• **Contesting Record Procedures:** Identifies the rulemaking for seeking a change to a systems notice based on factual inaccuracy of data.

• **Record Source Categories:** Identifies where the information is obtained (i.e., individual; personnel file; etc).

• **Exemptions claimed for the system:** Identifies what information may be exempt from disclosure.