The New Federal ID Card: Privacy Implications

Pam Dixon
Executive Director, World Privacy Forum

Homeland Security Presidential Directive12 Public Meeting

Washington, D.C., January 19, 2005

Privacy Frameworks

- Fair Information Practices.
- E-Government Act of 2002 (PIA).
- Privacy Act of 1974 (System of Records).
- OMB guidance (Memo 03-22; Memo 00-13; A-130, Capital Asset Plan and Business Case).
- FISMA (Federal Information Mgmt Security Act).

Privacy Risks

- "Mission Creep" for card use. Ex., NHIN use based on VA hospital use [1]? Proposed METRO use of card [2].
- Unique Card ID subject to same pressures and abuses as SSNs.
- Length and manner of storage/access for original source documents such as birth certificates.
- Tremendous risk with PII.

- Transactional data mining (How card was used by individuals or groups of individuals).
- Real time tracking (physical, computer use).
- Unauthorized use, access, disclosure, disruption, modification, or destruction.
- Data matching (SSN, Census, IRS, etc.)
- Inability to limit use by private sector.

- Background check implementation and application across agencies.

- Proposed use of the card for "long term visitors," others. LTV= Whom? (L.O.C. researchers? Surgeons called in as specialists for rare VA Hospital surgeries? What is the standard?)

- Proposed use of the card for press members, including White House Press Pool [3], is not appropriate and should be banned.

- Use of live test data by vendors.
- Lack of appeal and redress procedures.
- Lack of a specific plan for audit, access control, protocols, training, and other very basic privacy-protecting mechanisms.
- Lack of substantive PIA, Privacy Act compliance.

Privacy Impact Assesment

- Federal ID will span 24 agencies.
- Different cards (eg., VA Hospital compared to EEOC).
- Variations of collection of PII.
- Variations of definitions of card recipient.
- Data warehousing and access differences.

- PIA is already late and needs to be done immediately.
- PIA should be done by lead agency and be applied to all affected agencies.
- PIA needs to be published publicly before the first contract is signed.
- Must abide by the spirit of the law.

Required Elements of a PIA: (OMB Memo M-03-22)

- **What** information is to be collected.
- **Why** the information is being collected.
- **Intended uses** of the data.
- **With whom** the information will be shared.

- **What opportunities** individuals have to decline to provide (ie, where providing information is voluntary) or to consent to particular uses of the information, and how individuals can grant consent.

- **How** information will be secured (Administrative and technological controls).

- **Whether** a system of records is being created under the Privacy Act, 5 U.S.C. 552a.

Privacy Act

- A new System of Records has definitely been created.
- Federal Register notice for all agencies; PA compliance must be applied across all 24 agencies evenly.
- A system of this scope and impact needs an excellent, extremely thorough PA notice, no escaping via the "routine use" route.

Other Questions and Issues

- Security risks with the card relating to the technology.
- Legislation to strictly limit the use of the card. Needs to be a means for enforcing limitations of card use by non-governmental entities and for providing private right of action.
- Employee Privacy Training.
- Privacy Officer dedicated to this issue.

- Where are the specific, detailed audit and redress procedures across the board, from fair and even application of background checks to auditing procedures to monitoring expansion of uses?

- Strictly limit use of card and uses of card data within government, including transactional data. Must not be used for the NHIN, as purchase cards, etc.

- PA notice compliance on card application forms? I-9, other?

Resources

- E-Government Act of 2002 (Pub. L. 107-347), 44 U.S.C. 36.
- OMB Circular A-130, Management of Federal Information Resources, Appendix I, Federal Agency Responsibilities for Maintaining Records About Individuals.
- OMB Circular A-130, Management of Federal Information Resources, Appendix III, Security of Federal Automated Information Systems, February 8, 1996
- OMB Memo-03-22, OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002.
- Paperwork Reduction Act, 44 U.S.C. 35, and 5 C.F.R. Part 1320.8.
- Privacy Act of 1974, 5 U.S.C. 552a.
- VA Handbook 6300.4, Procedures for Processing Requests for Records Subject to the Privacy Act (PA); also VA HANDBOOK 6502.2, Privacy Impact Assessment Handbook.

Citations

- [1] "Department of Veterans Affairs to use IWS EPI Builder for AAIP Smart Card Initiative," Sept. 6 2004, Federal Computer Market Report.
- [2] "Transit Group Seeks Common Farecard System." (Standards). June 21 2004, Government Computer News. Jackson, William.
- [3] http://csrc.nist.gov/piv-project/workshop-Oct062004/presentations.html See Grance, Tim, p. 5. [last visited January 17, 2005].