Privacy Protection and the Common Identification Standard for Federal Employees and Contractors

Frannie Wellings
Policy Analyst
EPIC

January 19, 2005

epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

epic.org

- EPIC is a public interest research center in Washington, D.C. It was established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values.
- EPIC has done a great deal of work on Privacy Protection and identification including work on biometric passports, rfid smart cards, the use of the Social Security Number, National Identification proposals.
- http://www.epic.org/

Significance of Privacy Protections for the Federal Employee ID

- One of the functional objectives is to “Protect the privacy of the cardholder” (section 3.1).
- This proposal does not include adequate safeguards to accomplish this objective.
- At a minimum, Fair Information Practices could be a guideline for protection of employee information.
- Persistent identification raises additional risks that should be addressed

According to Fair Information Practices

- They have been the historical basis for privacy laws and industry codes of best practices
- Employees, Contractors, and other Data Subjects
  - must know that this record is being kept
  - must be able to find out what information is being gathered and retained and how it is used
  - must be able to correct the information held
- Their information should be used for only the purpose specified
- and it must be reliable and secure

Privacy Impact Assessment

- This proposal cries out for a Privacy Impact Assessment (PIA)
- It should be performed immediately
- Must be proactive: incorporate privacy protections into the decision making process rather than awkwardly and inefficiently adjust later
- PIA’s are now routinely required for federal record-keeping systems. Why shouldn't this particularly important for an ID proposal that is so controversial?

Source Documents Should not be Retained

- Applicant must submit two forms of identification from I-9, including a valid State or Federal government issued picture ID.
- The Authorizing Official sends photocopies to Registration authority and Issuing authority.
- Registration authority maintains the copies and results of the background check.
- Issuing authority will photograph Applicant and retain copy.

Data Minimization

- The extent of data collected and retained should be as minimal as possible.
- Proposed data collected at application includes: full name, address, marital status, date of birth, Federal designation, sponsor identity and biometric information.
- Storage of data should be minimal.
- The data stored actually on the card includes: personal information, certificates, the Personal Identification Number, and biometric data.
- The applicant may include pay grade and rank as “optional” visual information on their card.
- The military card will contain date of birth and social security number as visual information on the card.
- This is a lot of information!
- Data minimization would reduce the likelihood that the card will be used for unrelated or potentially risky purposes.

Contactless Cards

- Contactless cards pose a real security problem.
- They allow for remote / covert monitoring.
- They are insecure if not encrypted.
- This could allow others to remotely monitor.

Security of Backend Information

- Security of this information requires security and privacy training of all employees accessing, controlling, storing the data.
- Security requires oversight.
- There must be explicit policies limiting the use of the data, including private sector contractor access and use.
- Security of information across agencies still seems questionable.

Life of Information in Databases

- What happens to the information after the employee leaves or contractor finishes work?
- The PIV card is destroyed, but what about the rest of the information at the Registration Authority?
- The source documents and other documentation maintained by the Registration and Issuing Authorities could become a centralized bank of information.
- This information should be destroyed.

Mission or Function Creep

- How will all of this information be used? How will the public, the employees know how each agency is using this information?
- What will ensure that the agencies or contractors will not use the data for other purposes?
- What is the potential for tracking movement? There must first be explicit limitations on use.
- As the cardholder uses the card to access various areas, a record of these movements can be retained, creating a high volume of data about the movements of federal employees. This could be exploited.
- Unions have valid concerns

Mission or Function Creep

- We don’t even have to speculate about possible misuse, we have a concrete example of CAPPS II, as revealed by EPIC's efforts, to prove that in fact mission creep occurs.
- EPIC has shown through the FOIA that the passenger profiling system quickly morphed into a much broader program than terrorist screening.
- Will this type of identification creep into the private sector?

Who Will Be Required to Carry a Card?

- Federal employees
- US Contractors
- Visitors ?
- Foreign contractors
- The Press ???

Stranded

- Should the Employee be wrongly identified or not-identifiable, what are his/her methods of redress? There must be methods of redress put in place beforehand.
- What happens in a case of biometrics?
- With fingerprints for example - could have a correct original, but mistakes in matching
- And in the use of biometric facial imaging, while not the primary biometric in use here, it requires a degree of skill in capturing the image. The use of the technology remains inaccurate.
- And what happens in a case of identity theft?
- There must be privacy officers at all of these agencies.
- And there must first be legally enforceable rights.

Public Opinion of Identification Systems

- There is strong, historic opposition in the US to the use of a single identifier.
- Even though the SSN is widely used, the Privacy Act (section 7) makes clear that use should be limited, the trend in many institutions is to move away from a single identifier.
- Universities (such as Georgetown) are dropping the SSN as a student ID because of concerns that it contributes to identity theft.
- Microsoft's single sign-on service for the Internet, Passport, has collapsed because of the risks associated with a centralized credentialing system.

To Summarize

- There needs to be a Privacy Impact Assessment
- Need to Question the Scope of this System
- In order to really protect the privacy of Federal Employees who are dedicating themselves to public service, this type of proposal will require legislation enforcing their rights.

Further Information

- Workplace Privacy Page: http://www.epic.org/privacy/workplace/
- Biometrics Page: http://www.epic.org/privacy/biometrics/
- Passenger profiling: http://www.epic.org/privacy/airtravel/profiling.html/
- Privacy & Human Rights 2004 (for a comparative assessment of ID proposals)

- Questions? Contact Frannie Wellings at wellings@epic.org