# Privacy Implications of E-Authentication

HSPD-12 Public Meeting
Steve Holden
Department of IS
UMBC

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# Authentication Technologies Have Privacy Implications

- Note that *affecting* privacy is not always a *violation* of privacy
- Possibilities *exist* for affecting privacy in negative ways
  - RFID
  - PKI
  - Biometrics
- Challenge: Realize business value from e-government with e-authentication consistent with user values for privacy

UMBC
AN HONORS UNIVERSITY IN MARYLAND

# Code of Fair Information Practices

1. There must be no personal data record-keeping systems whose very existence is secret.
2. There must be a way for a person to find out what information about the person is in a record and how it is used.
3. There must be a way for a person to prevent information about the person that was obtained for one purpose from being used or made available for other purposes without the person's consent.
4. There must be a way for a person to correct or amend a record of identifiable information about the person.
5. 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 misuses of the data.

From: U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973).

# General Privacy Implications of Authentication

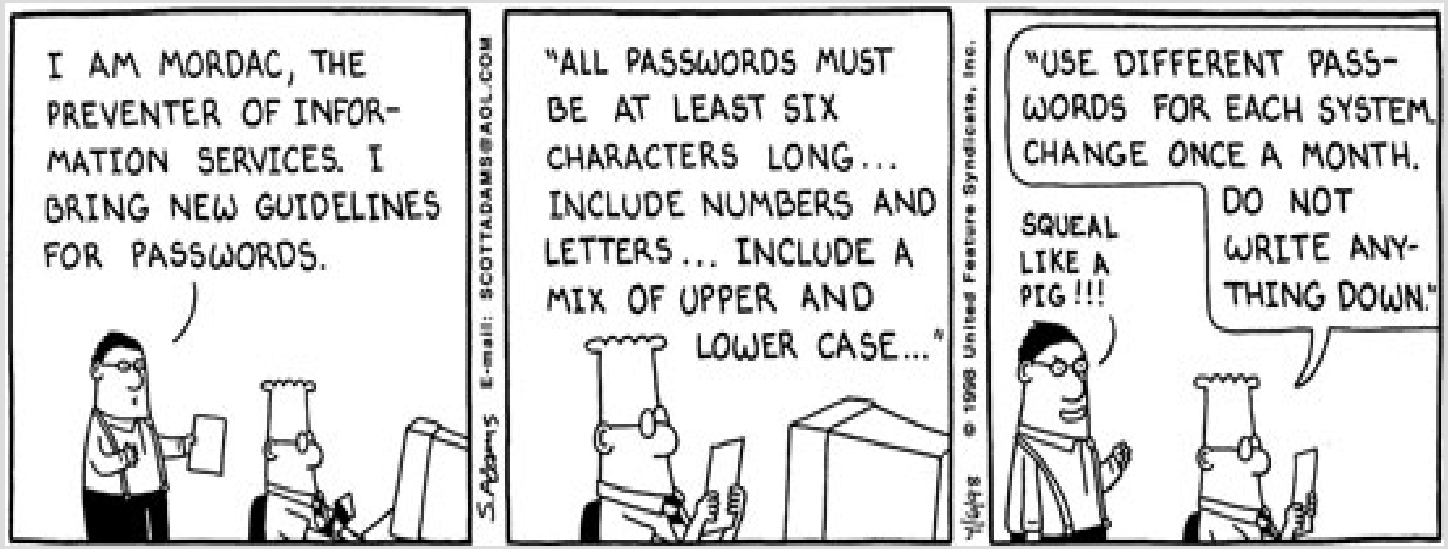
- Terminology is central
- Authentication can implicate privacy – the broader the scope, the greater the potential privacy impact
- Using a small number of identifiers across systems facilitates linkage, affects privacy
- Incentives to protect privacy are needed
- Minimize linkage and secondary use
- Usability is important for privacy and security

From NRC Report: Who Goes There? Authentication Through the Lens of Privacy

# National Research Council Report

- Toolkit with checklist of questions around four big design decisions
  - Attribute Choice
  - Identifier Choice
  - Identity Selection
  - Authentication Phase
- Examine each decision against the four types of privacy implications
  - Information privacy
  - Bodily integrity
  - Decisional privacy
  - Communications privacy
- Q: Is this well understood enough to use?

# The Usability/Security Paradox



# PIA Background

- Why?
  - E-Government Act of 2002
- What?
  - An analysis of how individually identifiable information is handled
  - An assessment of privacy risks in association with information systems
  - A means to ensure compliance with laws and regulations governing privacy
  - Integrates privacy protection into system life cycle
- How?
  - Models from IRS, Canada, New Zealand

# How to Do a PIA?

- What identifiable information will be collected?
- Why the information is to be collected?
- How the information will be used?
- With whom the information will be shared?
- What opportunities do individuals have to object to the collection of information about themselves?
- What information is provided to the individual and format?
- What are the  administrative, physical, and technical controls?

**Q: Is this sufficient to evaluate privacy impact of systems required by HSPD-12?**

Example from DOD TRICARE Management Activity Privacy Office

# Comparison of Privacy Impact Analysis and NRC Toolkit

| | PIA | NRC Toolkit |
|---|---|---|
| Scope of Analysis | Broad | Narrow |
| Level of Abstraction | Medium to Low | High |
| Complexity | Medium | High |
| Focus of Analysis | Data, Technology and Business Process | Data and Technology |
| Timing | Before, During or After Development | Best Before or During Development |
| Manageability | High | Unknown |

# Final Thoughts

- Privacy Impact Does Not Mean Privacy Invasive
- Analytical Tools Available
- Plan for Privacy and Usability Early in Life Cycle
- Communicate with Users

UMBC
AN HONORS UNIVERSITY IN MARYLAND