

# Privacy Principles for RFID

Jim Dempsey  
Policy Director

Center for Democracy and Technology

Is It the Technology  
or  
Is It The Policy?

Is It the Technology  
or  
Is It The Policy?

It's Both

**ID in General**

**Unique Aspects of RFID**

# Foundation Already Laid

- DHS Data Privacy and Integrity Advisory Committee, Dec 2006
- GAO, “Info Sec: RFID Tech in the Fed Gov’t,” May 2005
- DHS IG, US-VISIT System Using RFID, June 2006
- IEEE-USA, “Developing Nat’l Policies for RFID,” Feb 2006

# PASSPORT



*United States  
of America*



# PRIVACY PRINCIPLES FOR IDENTITY IN THE DIGITAL AGE

Draft for Comment - Version 1.4

Center for Democracy & Technology - September 2007

## I. INTRODUCTION

### Intersection of Identity and Technology

How to create and manage individual identity is becoming a central challenge of the digital age. As identity-related initiatives are implemented in both the public and private sectors, individuals are being asked to identify themselves in some way with increasing frequency.

A major goal of many modern identity programs is to prevent illegal activity or enhance security, whether it be the security of our national borders, airplanes, workplaces, health records, or online transactions. However, the collection, storage, and disclosure of identity information can create risks to personal privacy and security. Poorly implemented identity systems can unnecessarily invade the privacy of innocent Americans, and can actually contribute to identity theft or weaken security.

Technologies – such as databases, machine-readable identification cards, and online accounts – are playing an ever more important role in identity systems. Identity-related technologies can help realize the potential of the digital age, whether by making e-

# Three Overarching Principles

- Diversity and decentralization
- Proportionality
- Privacy and security by design

# 8 Principles Based on FIPs

- Purpose Specification
- Limited Use
- Notice (Transparency)
- Individual Choice and Control
- Security
- Accountability
- Access
- Data Quality

# Less is (Usually) More

- Minimize info on the card
- The more info on the card, the more security is needed
- Largest privacy risk: It's not the "card," it's the backend database
- Therefore: minimize backend databases, minimize storage

# Moving Forward

- No ban on technology
- How to ensure consideration of the issues
- Technology assessment
  - Efficacy
  - How much data
  - How secure
  - “Backend”
- Government access standards