

**Midwestern Intergovernmental Audit Forum
Madison, Wisconsin
April 24, 2007**

Carole Doeppers, Data Privacy Consultant

- I. Data privacy at the intersection of technology and data handling practices
 - Benefits of technology are well understood: Efficiency, program effectiveness, convenience, public safety
 - Less attention has been paid to the downside of technology and its potential for harm
 - Why should you care about privacy....if you have “nothing to hide?”
 - Unwarranted surveillance
 - Data tracking over distance and time
 - Erosion of consent and awareness
 - Sale of personal information for profit
 - Concern over data integrity and inaccuracy
 - Lack of accountability and transparency
 - Proliferation of identity theft

- II. Privacy as a value and legal principle
 - Personal privacy centers on concepts of solitude, dignity, autonomy
 - Data privacy centers on personal control over how one’s own information is used, reused and potentially misused
 - Privacy is not explicitly mentioned in the US Constitution
 - Fourth amendment protects against unreasonable searches
 - Other amendments limit government intrusion into private lives
 - Privacy as a legal concept was first articulated by Supreme Court Justice Louis Brandeis as the “right to be let alone”

- III. Modern governmental bureaucracies have embraced information technologies uncritically
 - Growth of large scale data repositories
 - Computer matching and merging programs
 - Data mining
 - Creation of personal profiles and *data dossiers*
 - Integration and interconnection of large-scale information systems
 - Secondary use of personal information
 - Outsourcing and problems of maintaining confidentiality
 - Proliferation of government web sites
 - Law enforcement information sharing in the name of national security

- IV. FOIA versus privacy acts: competing and potentially conflicting values
 - Public records decision-making is complicated by complex record systems
 - Questions for consideration
 - Who has custody of integrated or shared records?

- Who should be responsible for data accuracy and integrity when records are integrated or posted on the Internet?
- What needs to be redacted when confidential information is merged with public information?
- Should data providers have any control over what and how much personal information is posted on a government web site?
- Should data providers be notified and/or allowed to opt-out when personal information is used for a secondary purpose?
- Should government web sites contain consolidated and/or customized information for the convenience of stake holders?
- Should sensitive information and unique identifiers be suppressed from public records and government web sites?

VI. Record security

- Record number of security breaches
 - Stolen or lost lap tops
 - Hacking and fraud
 - Theft of identity
- Impact on public trust and acceptance of government data handling practices
- Resolutions to consider
 - Biometric identification
 - Authentication
 - Cryptography
 - De-identification
 - De-emphasis on Social Security Numbers