U.S. Government Privacy Laws

A. Privacy Definitions and Principles
   a. Privacy Definitions
      i. Privacy and personally identifiable information (PII)
      ii. Definition of PII
         1. Office of Management and Budget (OMB) Memorandum M-07-16: "Safeguarding Against and Responding to the Breach of Personally Identifiable Information"
         2. OMB Memorandum M-10-23: “Guidance for Agency Use of Third-Party Websites and Applications”
   b. Privacy Basics
      i. Privacy as a core value in U.S. government
         1. Confidence and trust
         2. Mission effectiveness
               1. Leadership
               2. Privacy risk management and compliance documentation
               3. Information security
4. Incident response
   a. OMB Memorandum M-07-16: “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”
   b. OMB Memorandum issued September 20, 2006: “Recommendations for Identity Theft Related Data Breach Notification”

5. Notice and redress for individuals

6. Privacy training and awareness

7. Accountability

3. Conflict/tension/intersection of privacy and national security
   c. Fair Information Practice Principles
      ii. Relationship to Organisation for Economic Co-operation and Development (OECD) Guidelines
      iii. Examples of Federal Agency approaches to FIPPs

B. The Privacy Act and the E-Government Act
   a. The Privacy Act of 1974 (as amended)
      i. Purpose and policy objectives
      ii. Scope and definitions
         1. Agency
         2. Individual
         3. Record
         4. System of records
            a. Retrieval requirement
            b. System of Records Notice (SORN)
               1. Publication
               2. Elements
      iii. No disclosure without consent
         1. 12 exceptions
            a. Internal disclosures
            b. External disclosures
               1. Routine uses
               2. Other authorized disclosures
               3. Accountings
iv. Agency requirements
   1. Collection
   2. Maintenance
   3. Notice
   4. Record standards
   5. Access and amendment
   6. Safeguards
   7. Contractors
   8. Computer matching
   9. Reporting
   10. Social Security numbers

v. Exemptions

vi. Civil remedies and criminal penalties

vii. Office of Management and Budget
   2. OMB, "Privacy Act Implementation, Guidelines and Responsibilities", 40 Fed. Reg. 28,948 (1975), and supplemental guidance

   ii. OMB Memorandum M-10-22: "Guidance for Online Use of Web Measurement and Customization Technologies" (June 25, 2010)
   iii. OMB Memorandum M-10-23: "Guidance for Agency Use of Third-Party Websites and Applications" (June 10, 2010)

iv. Website privacy policy (Section 208)
   1. OMB Memorandum M-99-18, Attachment: "Guidance and Model Language for Federal Web Site Privacy Policies"
   2. OMB Memorandum M-03-22, Appendix A, Section III.: "Privacy Policies on Agency Websites"
   3. Contents of privacy policy
      a. Consent to collection and sharing
      b. Requirements on agencies
      c. Rights of individuals
      d. Comply with the Children's Online Privacy Protection Act (COPPA)
v. Modifications to prior OMB guidelines
   1. Notice options
   2. Machine-readable privacy policy
vi. Privacy Impact Assessments (PIAs)
   1. When required
   2. Timing
   3. Content
   4. Exceptions
      a. National security systems
      b. Systems previously assessed under a PIA
      c. Internal government operations
      d. Systems collecting non-PII
         1. Government websites
   5. PIAs versus SORNs
   6. Publication requirements
   7. Reporting requirements
   8. Requirements for social media and third-party websites
      (adapted PIAs)
   9. Relationship to the Privacy Act of 1974
      a. OMB Memorandum M-06-15: "Safeguarding Personally Identifiable Information"
      b. OMB Memorandum M-06-16: "Protection of Sensitive Agency Information"
C. Other Laws and Regulations Affecting U.S. Government Privacy Practice
   a. Consolidated Appropriations Act of 2005
      i. Chief privacy officer and audit provisions
      ii. OMB Memorandum M-05-08: "Designation of Senior Agency Officials for Privacy"
      i. Federal agency responsibilities
         1. Agency program
         2. Agency reporting
         3. Performance program
      ii. System vs. enterprise compliance
         1. PIA versus security assessment and authorization
2. National Institute of Standards and Technology (NIST) risk management framework
   a. SP 800-122: "Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)"
   b. SP 800-53: "Recommended Security Controls for Federal Information Systems and Organizations"
   c. SP 800-64: "Security Considerations in the System Development Life Cycle"
   e. FIPS 200: "Minimum Security Requirements for Federal Information and Information Systems"

   iii. OMB reporting instructions for FISMA

   c. The Freedom of Information Act of 1974 (FOIA)
      i. Publicly available information
         1. Regulations
      ii. FOIA requests
         1. Interface with the Privacy Act
         2. Exemptions under the Act
         3. Exclusions under the Act

      i. OMB Memorandum, April 7, 2010: "Social Media, Web-Based Interactive Technologies, and the Paperwork Reduction Act"

   e. The Data Quality Act of 2002
      i. OMB guidance
      ii. Agency requirements
      iii. Administrative mechanisms
      iv. Periodic reporting

   f. Federal open meetings laws
      i. Federal Advisory Committee Act (FACA)
      ii. Government in the Sunshine Act

   g. Open Government Directive
      i. OMB Memorandum M-10-06

   h. Confidential Information Protection and Statistical Efficiency Act of 2002 (CIPSEA)
      i. Controlled Unclassified Information (CUI) Office Notice 2011-01: Initial Implementation Guidance for Executive Order 13556
D. Privacy and the Federal Government Intelligence Community
   a. The Federal Intelligence Community and the Information Sharing Environment (ISE)
      i. ISE Privacy Guidelines
      iii. Title VIII: Privacy and Civil Liberties
           1. Section 801: Modification of Authorities Relating to Privacy and Civil Liberties Oversight Board
           2. Section 802: Department Privacy Officer
           3. Section 803: Privacy and Civil Liberties Officers

E. Other Federal Information Privacy Laws and Authorities Affecting Government Practice
   a. Laws affecting both the public and private sectors
      i. Family Educational Rights and Privacy Act of 1974 (FERPA)
      ii. Health Insurance Portability and Accountability Act of 1998 (HIPAA)
      iii. Health Information Technology for Economic and Clinical Health Act of 2009 (HITECH)
      iv. Children’s Online Privacy Protection Act of 2000 (COPPA)
      v. Financial Services Modernization Act of 1999 (“Gramm-Leach-Bliley Act” or GLBA)
      vi. Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003 (The Red Flags Rule)
   b. Laws Limiting Government Access
      i. Bank Secrecy Act of 1970
      ii. Foreign Intelligence Surveillance Act of 1978 (FISA)
      iii. Right to Financial Privacy Act of 1978
      iv. Electronic Communications Privacy Act of 1986 (ECPA)
      v. Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001 (USA-PATRIOT)
      vi. The Real ID Act of 2005
      vii. Cable Communications Policy Act 1984

II. U.S. Government Privacy Practices
   A. Privacy Program Management and Organization
      a. Program development
         ii. Program elements
b. Program management
   i. FISMA model
   ii. Federal Enterprise Architecture Security and Privacy Profile
   iii. The Annual OMB Memorandum on Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management

c. Federal agency responsibilities
   i. All agencies
   ii. Department of Commerce
   iii. Office of Personnel Management (OPM)
   iv. National Archives and Records Administration (NARA)
   v. Office of Management and Budget (OMB)

d. Protecting PII
   ii. The President’s identity task force report
   iii. OMB Memorandum M-07-16: “Safeguarding Against and Responding to the Breach of Personally Identifiable Information”

e. U.S. Government workforce management
   i. Workforce hiring considerations
      1. Office of Personnel Management
         a. OPM Memorandum: “Guidance on Protecting Federal Employee and Social Security Numbers and Combating Identity Theft” (June 18, 2007)
      2. Background screening and investigations
         a. Levels of screening
         b. Financial and medical records
      3. Monitoring all use of Federal Government Agency Networks
      4. Surveillance in Federal Government Buildings
   ii. Federal identity management and authentication
      2. Federal Identity, Credential and Access Management (FICAM)

f. Privacy policy enforcement
   i. Single or multiple policies for each agency
   ii. Sample approaches
1. Census Bureau
2. Internal Revenue Service (IRS)
3. Department of Homeland Security (DHS)
4. Department of Defense (DoD)

B. Records Management
   a. Management Process
      i. OMB Circular A-130: "Management of Federal Information Resources"
   b. Record retention
   c. Inter-agency sharing of personal data
      i. OMB Memorandum M-11-02: “Sharing Data While Protecting Privacy”
      ii. OMB Memorandum M-01-05: "Guidance on Inter-Agency Sharing of Personal Data—Protecting Personal Privacy”
      iii. OMB Memorandum M-04-26: "Personal Use Policies and 'File Sharing’ Technology”
   d. Common Rule for Protection of Human Subjects
      i. Institutional review boards (IRBs)
   e. Disclosure of PII for statistical or research purposes
      i. Government source to third parties
      ii. Disclosure avoidance and the challenge of “big data”
      iii. CIPSEA impact for selected agencies

C. Auditing and Compliance Monitoring
   a. Auditing
      i. Pre-audit (e.g. PIA)
      ii. Post-audit (e.g. periodic review of disclosure audit trails)
      iii. Assessments vs. audits
   b. Compliance monitoring and reporting
      i. Office of Management and Budget (OMB)
      ii. Inspector General (IG)
      iii. Government Accountability Office (GAO)
      iv. Department of Justice (DOJ)
      v. Department of Health and Human Services (HHS)
         1. Office for Civil Rights (OCR)