

Author(s): David A. Wallace and Margaret Hedstrom, 2009

License: Unless otherwise noted, this material is made available under the terms of the **Creative Commons Attribution Noncommercial Share Alike 3.0 License**:
<http://creativecommons.org/licenses/by-nc-sa/3.0/>

We have reviewed this material in accordance with U.S. Copyright Law **and have tried to maximize your ability to use, share, and adapt it.** The citation key on the following slide provides information about how you may share and adapt this material.

Copyright holders of content included in this material should contact open.michigan@umich.edu with any questions, corrections, or clarification regarding the use of content.

For more information about **how to cite** these materials visit <http://open.umich.edu/education/about/terms-of-use>.

Citation Key

for more information see: <http://open.umich.edu/wiki/CitationPolicy>

Use + Share + Adapt

{ Content the copyright holder, author, or law permits you to use, share and adapt. }



Public Domain – Government: Works that are produced by the U.S. Government. (USC 17 § 105)



Public Domain – Expired: Works that are no longer protected due to an expired copyright term.



Public Domain – Self Dedicated: Works that a copyright holder has dedicated to the public domain.



Creative Commons – Zero Waiver



Creative Commons – Attribution License



Creative Commons – Attribution Share Alike License



Creative Commons – Attribution Noncommercial License



Creative Commons – Attribution Noncommercial Share Alike License



GNU – Free Documentation License

Make Your Own Assessment

{ Content Open.Michigan believes can be used, shared, and adapted because it is ineligible for copyright. }



Public Domain – Ineligible: Works that are ineligible for copyright protection in the U.S. (USC 17 § 102(b)) *laws in your jurisdiction may differ

{ Content Open.Michigan has used under a Fair Use determination. }



Fair Use: Use of works that is determined to be Fair consistent with the U.S. Copyright Act. (USC 17 § 107) *laws in your jurisdiction may differ

Our determination **DOES NOT** mean that all uses of this 3rd-party content are Fair Uses and we **DO NOT** guarantee that your use of the content is Fair.

To use this content you should **do your own independent analysis** to determine whether or not your use will be Fair.

SI 655

Management of Electronic Records

Week 9

Sorting Out Contradictions:
Freedom of Information, Privacy, Security
& Accountability
March 23, 2009

OUTLINE

- Accountability and Transparency
- Accountability and Transparency Enhancers
- Accountability and Transparency Constraints

Accountability and Transparency

- **Accountability:** Based on the principle of access to information
- **Transparency:** Based on the practice of making information available in a way that is complete, accurate, understandable, and discoverable (visible)

Enhancers

- Voluntary Reporting
 - Global Reporting Initiative
 - Voluntary Posting of Information
- 3rd Party Reviews (e.g. Consumer Reports)
- Posting or dissemination of information required by law (adverse drug reactions, truth in advertising, “this call may be monitored”)
- Rights and procedures to request access to information (investor profiles, FOIA)
- Technological, organizational, and institutional safeguards (Meijer)

Government Information

- Freedom of Information Act (FOIA)
- Privacy Act
- Federal Register (Administrative Procedures Act)
- Open Meetings Laws (FACA; Sunshine in the Government Act)
- Conflict of Interest Statements
- Financial Disclosures for Political Appointees and some Civil Servants (Ethics in Government Act)
- Whistleblower Protection Act of 2007

(Vaughn)

Freedom of Information Act (FOIA)

- Enacted in 1966 and amended in 1974, 1986 and 1996
- Scope: Documents held by agencies of the executive branch of the US government
- Excludes Documents of
 - Elected Officials
 - the Federal Judiciary
 - Private Companies or Persons (including grantees and contractors)
 - State or Local Government

FOIA: Scope

- Existing records (regardless of form) in the possession [control] of the agency
- Requests must reasonably describe the records being sought
- Final decisions and policy recommendations
- Any requestor has standing

FOIA Exemptions

1. Classified documents (more later)
2. Internal personnel rules and practices
3. Information exempt under other laws
4. Confidential Business Information (a.k.a. trade secrets)
5. Internal government communications
6. Personal privacy (more later)
7. Law enforcement
8. Financial institutions
9. Geological information

FOIA Issues 1...

- Delays in responses to requests
- Denial of fee waivers
- Frivolous use of exemptions
- Expansion of exempt categories (sensitive security information; critical infrastructure)

FOIA Issues 2...

- Interrelated and Recurring Problems
 - Agency records management conditions
 - Antagonism towards FOIA by top agency officials, agency FOIA staff, and other federal employees
 - FOIA language provides high implementation discretion > ambiguity and inconsistency in interpretation and implementation
 - As FOIA matured its administration became more complex and courts became a significant venue in shaping administration and meaning

(Roth; Relyea)

EFOIAA of 1996 1...

- **Computer oriented amendments**
 - Computerized information applicable
 - Electronic reading rooms
 - Requester can receive response in desired form or format if "readily reproducible" or achievable within "reasonable efforts"
 - Agencies must apply "reasonable efforts" when searching electronic records
 - When "technically feasible," agencies are to note redactions on electronic releases
 - Each agency is to make available "an index of all major information systems of the agency and...a description of all major information and record locator systems maintained by the agency."

EFOIAA of 1996 2...

- **Administrative amendments**
 - Time limits
 - Multi-track processing and track negotiation
 - Expedited processing
 - Backlog and processing new requests (agencies can not use existing backlog as an excuse for not processing new requests)
 - Volume estimations for denied materials
 - Annual reporting reconfigured



Office of the Attorney General

Washington, D.C. 20530

March 19, 2009

© PD-GOV

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM:  THE ATTORNEY GENERAL

SUBJECT: The Freedom of Information Act (FOIA)

A Presumption of Openness

As President Obama instructed in his January 21 FOIA Memorandum, “The Freedom of Information Act should be administered with a clear presumption: In the face of doubt, openness prevails.” This presumption has two important implications.

FOIA Is Everyone’s Responsibility

Application of the proper disclosure standard is only one part of ensuring transparency. Open government requires not just a presumption of disclosure but also an effective system for responding to FOIA requests. Each agency must be fully accountable for its administration of the FOIA.

I would like to emphasize that responsibility for effective FOIA administration belongs to all of us—it is not merely a task assigned to an agency’s FOIA staff. We all must do our part to ensure open government. In recent reports to the Attorney General, agencies have noted that

Privacy Act

- Scope:
 - Personal information maintained by the Executive Branch of the US Government (including records maintained by contract on an agency's behalf)
 - US Citizens and permanent residents
 - Records maintained in a "system of records" (e.g. a system where information is retrieved by personal identifiers)

Privacy Act Requirements

1. Individual have a right to see and copy records about themselves
2. Agencies must publish notices describing all "systems of records"
3. Agencies must make reasonable efforts to maintain accurate, relevant, timely and complete records about individuals
4. Information collected for one purpose cannot be used for another purpose (w/o consent of the subject)
5. Legal recourse

Privacy Act Exemptions 1...

- All records maintained by the CIA
- Criminal Law Enforcement Agencies
 - Information compiled to identify individual criminal offenders
 - Criminal investigatory records
 - Reports identifiable to any individual from arrest to release from supervision

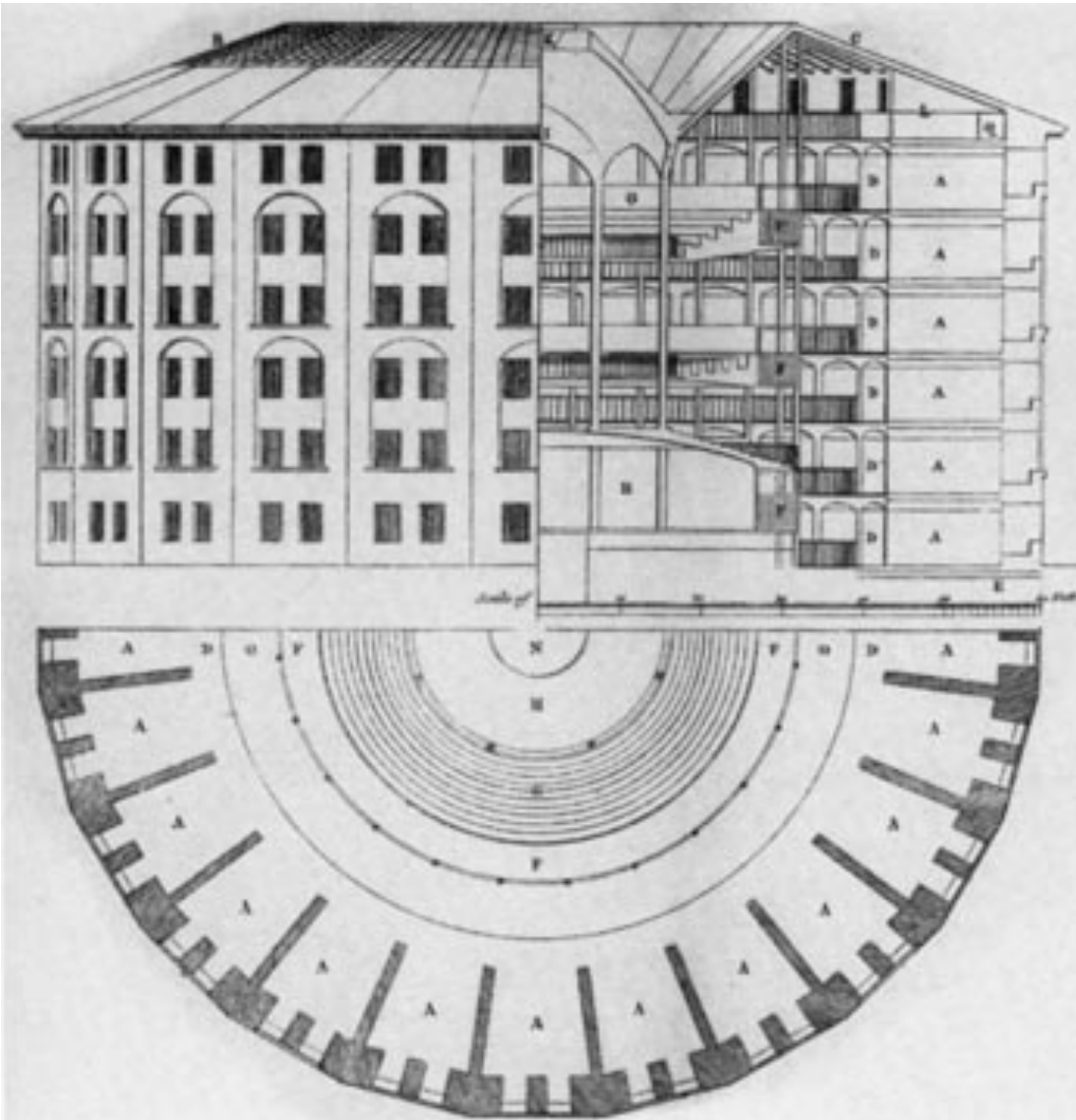
Privacy Act Exemptions 2...

1. Applicants for federal civil service positions
2. Classified records (more later)
3. Law enforcement investigatory material
4. Systems of records providing protective services (protect President)
5. Systems of records required by statute solely for statistical purposes (census records)
6. Information provided by a confidential source
7. Evaluation material for promotion in the armed services
8. Medical Records
9. Litigation Records

Panopticon revisited: accountability through transparency? technotyranny?

© PD-EXP

Jeremy Bentham ([Wikimedia Commons](#))



See:

<http://www.searchsystems.net/>

<http://www.choicepoint.com/>

<http://www.narus.com/>

<http://verint.com/>

Contentious Issues

- Unwarranted invasion of privacy
- Classified Documents

<http://www.pbs.org/wgbh/nova/spyfactory/>

Classified Documents

- Justification: to protect information from being used to damage or endanger national security.
- Levels of Classification:
 - Top Secret (exceptionally grave damage)
 - Secret (serious damage)
 - Confidential (damage)

Allowable categories

- (a) military plans, weapons systems, or operations
- (b) foreign government information
- (c) intelligence activities (including special activities), intelligence sources or methods, or cryptology;
- (d) foreign relations or foreign activities of the United States, including confidential sources
- (e) scientific, technological, or economic matters relating to the national security
- (f) programs for safeguarding nuclear materials or facilities
- (g) vulnerabilities or capabilities of systems, installations, infrastructures, projects, plans, or protection services relating to the national security
- (h) weapons of mass destruction

Authority to Classify Documents

- Classification and Declassification is governed by Executive Order
 - EO 13292 (March 2003)
 - Amends EO 12958 (1995)
- Clinton Administration 19 offices and agencies were authorized to classify documents
- Bush Administration added HHS, EPA, & Agriculture; OSTP upgraded to Top Secret

Declassification

- Automatic Declassification
 - Clinton EO: Documents more than 25 years old are automatically declassified unless the classification authority can demonstrate need to retain classification
 - Bush EO: Extended deadline for systematic review to Dec. 2006
- FOIA Request
- Mandatory Declassification Review Requests

Patriot Act

- Passed in wake of 9/11
- Break down historical barriers between domestic law enforcement and foreign intelligence
- Impact on government collection of PII via ELSUR
 - Altered 4th amendment protections (probable cause search warrants; unreasonable search and seizure)
 - “significant” to purpose of investigation
 - Records = any tangible information object
 - Secrecy clause = gag order
 - Changes to scope of wiretaps
 - Email and vmail surveillance
 - Increased sharing of information between agencies
- Implementation opaque but some indicators arising
(Jaeger, Bertot, McClure)

Concluding thought ala Alan Westin

- Totalitarian governments:
 - collect a lot of information on citizens with no/limited access rights
- Democratic governments:
 - limits on collection of personal information and broad access to information on government actions
- Access and privacy [and security] intertwined in democratic accountability and transparency