

# Policy and Privacy

---

Merri Beth Lavagnino, M.L.S., CIPP  
Chief Information Policy Officer  
Indiana University

EDUCAUSE CAMP  
June 20, 2008



**INDIANA UNIVERSITY**

**UNIVERSITY INFORMATION POLICY OFFICE**

Information and Infrastructure Assurance



INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance





INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

**“Plague [on] your  
policy!”**

William Shakespeare,  
British dramatist, poet (1564–1616)



INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance





INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

# POLICY



- Strategic direction/  
operating philosophy
- Public policy
- Institutional policy



## What should my policy do?


- Outline the philosophies and values of the project, service, organization, or federation



## Why would I create a policy?

- When reasonable people disagree
- To guide in **thinking** when making decisions
- To correct repeated misbehavior
- When significant liabilities are identified
- To deal with external forces such as regulation or law



The background of the slide is a close-up, vertical view of intense flames. The fire is bright orange and yellow at the base, transitioning to a darker red and black at the top. The flames are dynamic and appear to be rising. The text is centered over this background.

# **Super Hot Data Elements**

The background of the entire slide is a close-up, high-contrast image of flames. The flames are primarily orange and yellow at the bottom, transitioning into darker reds and blacks towards the top. The texture is highly detailed, showing the movement and intensity of the fire.

**Social Security number**

**Account number, credit card number, debit card number, security code, access code, or password of an individual's financial account**

**Health, medical, or psychological info**

**Driver's license number or identification card number**



## Other possibly hot data...

- Passwords
- Student records and grades
- Data classified by the institution/state at the highest risk levels
- Non-anonymized human subjects research data
- Trade secret data
- Birth date
- Mother's maiden name



## Where does the policy apply?

- Federation level
- Institution level
- Service level



**INDIANA UNIVERSITY**

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

# **A few real-life stories...**



“A policy is a temporary creed liable to be changed, but while it holds good it has got to be pursued with apostolic zeal.”

*Mohandas K. Gandhi,  
Indian political and spiritual leader (1869–1948)*



"It is always the best policy to speak the truth, unless, of course, you are an exceptionally good liar."

*Jerome K. Jerome,  
British author (1859–1927)*





INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance







INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

# PRIVACY



## Privacy definition

“Privacy is the claim of individuals, groups or institutions to determine for themselves when, how, and to what extent information about them is communicated to others.”

*Alan Westin: Privacy & Freedom, 1967*



## But, it's a moving target...

“Each individual is continually engaged in a ***personal adjustment process*** in which he balances the desire for privacy with the desire for disclosure and communication.”

*Alan Westin: Privacy & Freedom, 1967*



“An American has no sense of privacy. He does not know what it means. There is no such thing in the country.”

*George Bernard Shaw,  
Irish dramatist and socialist (1856-1950)*



## In the U.S.A...

- 1974 - Privacy Act
- 1996 - Health Insurance Portability and Accountability Act (HIPAA)
- 1999 - Gramm-Leach-Bliley Financial Services Modernization Act (GLBA)
- 2002 - California's SB1386, covering personal data such as SSN
- 2008 - Nearly every state follows CA



## So let's talk about...

- Categories of privacy harms (4)
- Fair information practice principles (5)



# 1. Intrusions

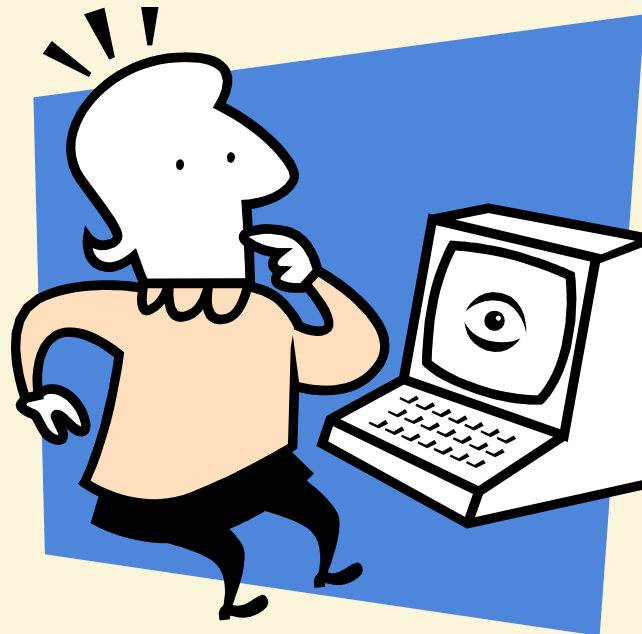
- “They” come into “your” space and contact you, or tell you what to do!





## 2. Information Collection

- “They” watch what “you” are doing, more than they should!







## 3. Information Processing

- “They” have a lot of data about “you”, and they do things with it!





## 4. Information Dissemination

- “They” disclose data about “you”, perhaps more than you think they should!





## Fair Information Practice Principles

- From the Federal Trade Commission (FTC), whose charge is to protect America's consumers
- “Five core principles of privacy protection”



# 1. Notice/Awareness

- Users should be given notice of your information practices, in order to make an informed choice about whether to provide information.



## 2. Choice/Consent

- Users should be given options as to how any personal information collected from them may be used.



### **3. Access/Participation**

- Users should be given access to the data held about them, and ability to contest that data's accuracy and completeness.



## 4. Integrity/Security

- Data should be secure and accurate.



## 5. Enforcement/Redress

- There should be a mechanism in place to enforce fair information practices, and it should include appropriate means of recourse by injured parties.





INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

# WHAT'S NEXT?



## Some general principles emerge

- Three categories of data security measures:
  - Administrative (policies and procedures and sanctions for violations)
  - Physical (locks, keycards, physical barriers to data)
  - Technical (passwords, encryption, etc.)
- Continuing assessment and adjustment of security measures in light of own and similar others' experience
- Periodic monitoring and testing of security measures
- Education of people handling SUPER HOT and HOT data on their roles and obligations
- Appropriate security and confidentiality obligations imposed on third parties with whom we share data



## Think about what you are doing

- Do we really need to collect/maintain/use/share super hot data, hot data, or other sensitive data?
- Are there less sensitive alternatives that would accomplish our objectives?
- If not, is access limited to just those who need to see it? Is access terminated for someone whose role changes and who no longer needs it?
- Do we understand exactly how and where the data is being collected, used, shared, and stored? Could we diagram and explain this if asked?
- Do we provide clear training and guidance for people handling sensitive data? Do we train them when new, and do we have adequate refresher training?



## Still thinking...

- Do we have a retention schedule that allows for secure destruction of data when no longer needed?
- Do we provide appropriate notice to our users before we collect data from them?
- Do we have users opt-in, instead of opt-out?
- Can a user find out what we store and use about them?  
Can they check it and correct it or complete it?
- Can a user indicate that they no longer wish to use the service, and have their data deleted?
- Do we make it clear where to report privacy harms or other issues? Do we investigate reports?



## Document what you are doing

- Pull together your project, service, or federation leaders, and outline your basic philosophies and values in one or more simple policies.
- When you make decisions based on those philosophies and values, document them as practices or procedures. Keep updating these as you keep making decisions.



## Document what others are doing

- Ensure that agreements with those you share data with (especially SUPER HOT and the just HOT), go through your official contracting unit:
  - To ensure appropriate due diligence on privacy/security issues
  - To ensure appropriate privacy/security obligations imposed on others



## Contract language to consider

- Use of data limited to purpose of agreement
- Implementation of adequate safeguards
- Secure return/destruction at end of performance
- Prompt notice of breach and cooperation with institution's response to breach
- Reimbursement of costs incurred by institution in event of breach
- Defense/indemnity of institution in event of third party claims related to breach



INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance







INDIANA UNIVERSITY

UNIVERSITY INFORMATION POLICY OFFICE

Information and Infrastructure Assurance

