*LISA Invited Talk*

# *Logging and Monitoring: How, Why, and When*

*30 October 1997*

Joseph M. Saul
ITD Office of Policy Development & Education
University of Michigan
*jmsaul@umich.edu*

# *Outline*

- Striking a Balance
- The Legal and Policy Environment
- The Data Vault
- Classifying Information
- Important Decisions

# Logging & Monitoring: *Striking a Balance*

- Needs of the **System Administrator**
- Needs of the **Users**
- Needs of the **University**

# Needs of the System Administrator

- Keep things running smoothly
- Be able to investigate security incidents
- Discourage wrongdoing

# Needs of the Users

- Have usable service
- Privacy (not just from intruders, but from the authorities as well)
- Know what’s going on

# Needs of the University

- Comply with applicable laws
- Protect its property
- Protect its data
- Maintain free exchange of ideas and open communication

# *The Legal and Policy Environment*

- What should we look at?
- What should we keep, and for how long?

# *What should we look at?*

## Laws

*Directly Relevant*

- Electronic Communications Privacy Act (ECPA)
- Family Educational Rights and Privacy Act (FERPA)

*Relevant by Analogy*

- Video Rental Privacy law
- Library privacy laws
- a host of others…

# University Policies — UM for Example

- SPG 601.07, “Proper Use of Information Resources, Information Technology, and Networks”
- SPG 601.11, “Privacy of Electronic Mail and Computer Files”

# *What should we keep, and for how long?*

## Laws

- Freedom of Information Act (FOIA)
- Civil discovery
- State records laws

# University Policies — UM for Example

- SPG 601.08-1, “Identification, Maintenance, and Preservation of Electronic Records created by the University of Michigan”

# *The Data Vault*

…implicates all of the areas of law discussed, plus:

- Copyright law
- Search and Seizure
- Human research regulations
- First Amendment ("chilling effect")

# What about your procedures?

# *Classifying Information*

- By Sensitivity
- By Availability

# By Sensitivity

1. No personally identifiable information

2. No personally identifiable information by itself, but can combine with other material to identify

3. Access information (where you logged in, etc.)

4. Transactional information (what you did/looked at/ who you emailed)

5. Contents of your communications

# By Availability

1. Publicly-available information (i.e. **`ps`** or **`who`** results)

2. Linked publicly-available information (can be far more intrusive) (Traffic Analysis)

3. Private information

# *Important Decisions*

- Why are you monitoring and logging?
- What are you going to monitor and log?
- Are you going to use the logs proactively, or as a means of investigating after the fact?
- How will you protect the logs themselves from intruders?

- Who can look at the logs, for what purposes, and under what circumstances?

- How long are you going to keep the logs around?

- What should you tell your users about logging and monitoring?