ITPB Task Force on Privacy and Data Protection
Meeting Summary and Recommendations to ITPB

I. Summary of September 12, 2003 Meeting

Attendees:
Susan Abeles, Controller
Christine Borgman, Information Studies
Alfonso Cardenas, Computer Science
Dana Cuff, Architecture
Michael Curry, Geography
Jim Davis, Office of Information Technology
Chris Foote, Chemistry & Biochemistry
Mike McCoy, Medical Center
Lisa Spangenberg, Graduate Student Representative to ITPB
Kent Wada, Office of Information Technology
Esther Woo-Benjamin, recorder, Office of Information Technology

Absent: Sharon Farb, Library

Charge to Task Force

Propose a scope of work for a Privacy and Data Protection Board and membership for that board.

Discussion

Impetus for task force: Growth of records management systems (print and electronic) that contain personally identifiable data, and the increasing integration of these systems, without general principles for privacy and data protection in place.

Current UCLA Landscape

The University of California and UCLA have existing policies that address most individual types of data (e.g. medical, financial, student records, etc.) but do not have general principles in place that address privacy and data protection. Most general principles being implemented in government and business environments are based on guidelines set forth by the Organization for Economic Cooperation and Development (OECD) starting in the late 1970s. Some individual policies at UCLA, such as the Health Insurance Portability and Accountability Act (HIPAA) are based on the OECD guidelines. UCLA complies with privacy and data protection statutes and regulations and makes periodic reports to UCOP as requested, but no single point of contact exists on campus. At least 9 different bodies have responsibility for privacy
and data protection compliance but no mechanism exists for them to communicate
with each other.

Good privacy and data protection practices should bolster faith in the integrity of
UCLA as an institution that values the privacy of its students, faculty and staff. Good
practices also should help to avoid lawsuits and other potential negative effects of
poor records management practices.

Purpose of a UCLA Privacy and Data Protection Board

Such a board should establish and promulgate principles that UCLA, as an institution,
respects the privacy of individuals and takes action to protect privacy and ensure the
protection of data.

The board should establish UCLA principles aligned with OECD principles (e.g.
collection limitation, data quality, purpose specification, use limitation, security
safeguards, openness, individual participation, accountability).

The board should articulate principles that reflect institutional values and cultural
expectations of the University. Legal compliance should be viewed as a minimum
level (not a maximum) of privacy and data protection (e.g. SB1386 – being prepared
to make notification is the minimum requirement).

UCLA should take a proactive role in education; develop training and awareness
program (some abuses are due to lack of education); inform people about what
happens to data that is collected (i.e. purpose of collection, release of data, retention
of data, who has access, etc.); and make use of existing protections (e.g. California

Scope of a UCLA Privacy and Data Protection Board

Responsibility for privacy and data protection is best divided between two boards,
one that is advisory and one that provides a means of communication among
managers of operational records management systems. The Advisory Board will
advise the EVC, Academic Senate, and the Operational Board. The Operational
Board will assist and advise in implementing privacy and data protection guidelines
for individual systems and units. University of Michigan has a good model for this
approach: http://www.umich.edu/~sacua/clbprivacy.htm

The Advisory Board would have these roles:

Vet new records management systems to ensure compliance with guidelines; require
privacy impact (much like environmental impact) statement for new systems. The
board will need to determine when to evaluate projects, because distinguishing
between new systems and enhancements to existing systems may be difficult.
Advocacy on behalf of different groups (like a policy traffic director). The board will advise rather than enforce. It will assist in developing general campus-wide compliance policies but encourage decentralized implementation.

Take a pro-active rather than reactive approach. Activities include promoting educational activities, frequently-asked questions (FAQ) statements for systems, and minimum length records retention. Stay ahead of and pre-empt problems that will arise due to emerging technologies.

The Operational Board would have these roles:

Provide a forum for discussion among managers of records management systems. Assist in translating principles established by the advisory board into practice, as appropriate for individual systems. Document existing policies, procedures, practices, education/training and responsibilities. Assess whether a matrix approach for coordination is satisfactory or whether other models are needed (e.g., hierarchical structure, campus privacy officer).

**Membership of UCLA Privacy and Data Protection Board**

**Advisory Board:**

This is an advisory, coordinative and advocacy board like ITPB that establishes high level principles and works with the Operational Board toward a larger vision. Membership to include representatives from Academic Senate, Administration, Libraries, those about whom data is collected (the consumer voice), those who have expertise in privacy and data protection, and students. Reporting to EVC and Senate, with a dotted line to the ITPB. Membership should not exceed 15 persons.

**Operational Board:**

This is an operational board composed of current heads of bodies that have responsibility for privacy and privacy and data protection (e.g. HIPAA, Libraries, UC IT Policies, UCLA Records Manager/Information Practices Coordinator, Student Affairs etc.) to encourage communication between groups.

**II. Recommendations to ITPB**

1. **Establish a UCLA Privacy and Data Protection Advisory Board**

   - **Membership:** representatives from Academic Senate, Administration, Libraries, consumer voice, experts in privacy and data protection, students, and from Operational Board. Maximum 15 members.

   - **Purpose:** advise, coordinate, provide vision
• **Charge:**
  a. Establish high level principles for UCLA following OECD guidelines
  b. Articulate principles that reflect institutional values and cultural expectations of the University
  c. Vet new records management systems to ensure compliance with guidelines
  d. Promote communication to the UCLA community regarding privacy and data protection

• **Reporting:** EVC and Academic Senate, with dotted line to ITPB

2. **Establish a UCLA Privacy and Data Protection Operational Board**

• **Membership:** current heads of coordinate bodies that have responsibility for privacy and privacy and data protection (e.g. HIPAA, Libraries, UC IT Policies, Student Affairs, Records Management/Information Practices Coordinator, etc.).

• **Purpose:** encourage communication between these groups as a means to promulgate privacy and data protection principles and guidelines, and to implement practices in operational systems.

• **Charge:**
  a. Establish means of regular communication and coordination between officers and units responsible for systems that contain personally identifiable data.
  b. Assess whether a matrix approach for coordination is satisfactory or whether other models are needed (e.g., hierarchical structure, campus privacy officer).
  c. If a privacy officer is needed, develop job description and responsibilities.
  d. Document and evaluate existing operational policies, procedures, practices, education/training, and responsibilities
  e. Determine other activities required campus-wide and take action to implement recommendations.

• **Reporting:** Advisory board, with dotted line to ITPB