ROADMAP FOR THE UC PRIVACY AND INFORMATION SECURITY INITIATIVE

**CHARGE:**
**TO RECOMMEND:**
1. An overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;
2. Specific actions or phases needed to implement this framework as University policy;
3. Governance, implementation and accountability structures across the University with respect to privacy and information security; and
4. A formal ongoing process through which the University can examine and where necessary address through policy vehicles the technical and societal changes that have an impact on University policy and practice in the areas of privacy and information security.

**Recommendations must be directly able to help resolve situations such as:**

a. Is scanning of all outbound email for campus users desirable?

b. How should UC respond to a public records request similar to that received by the University of Wisconsin-Madison?

c. Should campus network traffic be made available for research purposes?

d. Is tracking of an individual’s use of a web site permissible?

President Yudof accepts Steering Committee recommendations (or not).

Implementation of recommendations begins if approval obtained.

---

**The Steering Committee develops recommendations for:**

**Privacy Framework**

1. Statement of community values
2. Governance
   - Organizational and accountability structures
   - A sustainable review and escalation process
3. Strategic direction for policies
4. Actions or phases needed to implement the framework above as University policy.
PROPOSED MODEL FOR A PRIVACY FRAMEWORK

SYSTEMWIDE PRIVACY BOARD

- Establishes charter for privacy boards (e.g., purpose, authority, responsibilities, membership)
- Considers new privacy issues for the system (escalated by campuses) at a strategic level
- Owners of the Toolkit: determines/recommends changes to the Toolkit if needed
- Coordinates consistency across the system

THE TOOLKIT is intended to allow campus privacy boards to reconcile issues and maintain consistency.

- Policies articulating factors and criteria used to evaluate individual situations by campus privacy boards
- Statement of community values used by campus privacy boards to help guide decisions when policy needs to be interpreted
- Criteria for review and escalation used by campus privacy boards to determine when a situation should be escalated to the systemwide privacy board
- Training and awareness materials for privacy board members

CAMPUS PRIVACY BOARDS

- Address most issues locally through use of the Toolkit
- Escalate new issues not addressed by the Toolkit to the systemwide board
- Organize to fit local culture and leverage existing structures (e.g., CECRCs)

Examples:
- UCLA – Advisory Board on Privacy and Data Protection, reporting to the EVC and Provost
- UCSD – Information Data Security and Privacy Council, a subcommittee of the CECRC and Health Sciences Privacy Board
- UCSC – (example) A standing subcommittee of the CECRC, convened as needed, collaborating with the Senate Committee on Faculty Welfare and Academic Freedom. Reports to the EVC, has academic and operational perspectives, coordinates with IT boards and risk management

BASIC FUNCTION AND LINKAGES

Each campus board is intended to address the vast majority of operational issues raised at a campus through use of the Toolkit. An issue not addressed by the Toolkit is escalated to the systemwide board for consideration. The systemwide board will make authoritative recommendations for changes to the Toolkit (community values, policies and/or review and escalation criteria) if appropriate and direct the local campus board to consider the issue in light of the recommendations.
STATEMENT

Academic and intellectual freedom are values of the academy that help further the mission of the University. These freedoms are most vibrant where individuals have autonomy: where their inquiry is free because it is given adequate space for experimentation and their ability to speak and participate in discourse within the academy is possible without intimidation. Privacy is a condition that makes these values possible.

The University recognizes that there is a constellation of values and of legal, policy, and administrative obligations that are always in play. Privacy is an important condition threaded throughout this constellation:

• ensuring an appropriate level of privacy through its policies and practices, even as interpretations of privacy change over time;
• nurturing an environment of openness and creativity for teaching and research;
• honoring its obligation as a public institution to remain transparent, accountable and operationally effective; and
• safeguarding confidential information and assets for which it is a steward.

CONTEXT

Mission first

• We teach, we do research, we perform public service (and many other activities).
• We are a community rather than corporation: we are 24x7, we have everything that a city has, we are always fluid and changing, we all have multiple roles.

Values that apply to the entire community

• Freedoms: academic, intellectual, of inquiry, of expression, to read, to read anonymously
• Respect for others’ communications and information
• Collegiality

Conditions that apply to the entire the community

We start with these conditions as premises, recognizing certain activities require special consideration:

• Privacy: The right to be let alone.
• Confidentiality: Not revealing sensitive information.
• Anonymity: The condition of not being identified/identifiable.
• Transparency: Ensure the community understands the “rules of the road” (e.g., social norms) and is aware of any limitations of privacy (notice of expectations).

FIRST PRINCIPLE

• The University does not access or monitor communications.

However, there are situations based on context (rather than on role such as “faculty” or “staff”) – such as regulatory environment, data involved and risk – where different conditions may or should appropriately apply.
ROADMAP FOR THE UC PRIVACY AND INFORMATION SECURITY STEERING COMMITTEE

AGENDA ITEMS TO DATE

|----------|----------|----------|----------|----------|
| • Introductions  
  • Review of charge  
  • Committee deliverables  
  • Provisional 18-month plan  
  • Privacy issues impacting UC  
  • Foundational questions  
| • Privacy in the UC context  
  • A proposed structure for UC privacy  
  • Draft UC privacy statement  
  • Draft UC principles for safeguarding privacy  
|  
|  
| • Report from the UCLA Privacy Board on a statement of community values and a governance model  
  • Scenarios  
  • Scaling the problem  
| • Revisiting the roadmap  
  • Governance organization  

Jun 2010  
Steering Committee appointed

Aug 2010  
Working Group formed
President Yudof accepts Steering Committee recommendations (or not). Implementation of recommendations begins if approval obtained.