UC PRIVACY AND INFORMATION SECURITY

STEERING COMMITTEE
OCTOBER 25, 2010
Agenda

1:00 Welcome
    pm Introductions
    Review of the Committee’s Charge
    A Provisional 18-Month Plan

1:30 Setting the Stage
    Privacy Issues Impacting UC

2:00 Determining the Path Forward
    Committee Deliverables
    Statement of Community Principles and Values
    Foundational Questions
    Proposal for 2010

2:50 Logistics

3:00 Adjourn
Welcome

Introductions
Review of the Committee’s Charge
A Provisional 18-Month Plan
Review of the Committee’s Charge

- ... to make recommendations for:
  - an overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;
  - specific actions or phases needed to implement this framework as University policy;
  - governance, implementation, and accountability structures across the University with respect to privacy and information security; and
  - 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.
A Provisional 18-Month Plan

Fall 2010 • Privacy issues impacting UC
• UC principles and values of community
• Foundational questions

Winter 2011 • Governance and accountability

Spring • A framework
• Statement of community principles and values
• Governance
• Accountability
• Policies

Summer • Break

Fall • Sustainable review process
• Implementation process

Winter 2012 • Recommendations
Setting the Stage

Privacy Issues Impacting UC
Movie

http://www.aclu.org/ordering-pizza
Privacy Issues Impacting UC

- Regulatory compliance
- Serious consequences of failure
- Financial and operational necessity
- Increased demand for data sharing
- Confidential institutional data
- Faculty and staff – between individuals and institutions
- Technology
- The expectations of individuals
- Research and innovation
- *In loco parentis*
Regulatory Compliance

- HIPAA
- FERPA
- Patriot Act
- California Information Practices Act
- FTC Red Flag Rules
- Federal Privacy Act (SSNs)
- PCI-DSS (Credit Cards)
- DOJ
- IRS
- Data Mgmt. Plans Mandated By Funding Agencies
- DMCA
- CMS
- GLBA
- Intellectual Property Protection
- California Public Records Act
- Clery Act
- E-Discovery
- Research Misconduct (e.g. human subjects)
- ADA
- Patriot Act
- IRS
- DOE
Best practices for compliance due diligence now sometimes requires preemptive measures rather than reactive corrective action, in contrast to the University’s current stance on civil liberty privacy (cf. UC stance on illegal file sharing).
Serious Consequences of Failure

- Data breaches: financial (notification expenses, fines, legal fees, productivity loss), reputational and legislative consequences
- **Virginia Tech tragedy**
- Regulatory investigations (e.g., by Cal/OSHA, OIG, FDA, OCR, …)
- Suspended research programs
- Potential loss of Federal financial aid funding (HEOA)
Financial and Operational Necessity

- Regents’ resolution on administrative efficiency
- Public transparency and accountability
- Marketing
- Development
- Outsourcing and the ubiquity of “free” Internet services
- Complexity and number of University policies related to privacy, information security and records management
- Incidental personal use
- **PCI banking status to accept credit cards**
- Role of “big brother” relating to employees (e.g., surveillance cameras)
Increasing Demand for Data Sharing

- Collect more, share more of what’s been collected
- By business, legislators, law enforcement, customers
  - Service provisioning (e.g., atyourservice.ucop.edu)
  - IT security, network management, audit, …
  - Health information exchange and networks
  - Tension between California legislature desires for reduced SSN use and increased analysis of student outcomes and accountability (requiring SSNs)
  - **California Public Records Act** requests
  - USA PATRIOT Act and National Security Letters
  - Open exchange of information and ideas
Confidential Institutional Data

- Institutional data beyond personal information that we may want to protect
  - Infrastructure plans
  - Computer security information
  - Intellectual property
  - Accreditation reviews
  - Campus directories
Faculty and Staff: Between Individuals and Institutions

- Faculty and staff have expectations as individuals, but are also expected to be institutional stewards
- Authority to access confidential data for work purposes versus for personal purposes (e.g., looking up one’s own records or those of family or friends)
- Clinical faculty are custodians of patient data as physicians, but want more access to data as researchers
  - Social media (e.g., Facebook) “friend” requests
  - Faculty as patients

**Blurring of personal and work lives**
- Use of personally owned devices in the workplace
- Use of institutional resources for (incidental) personal use
Technology

- The net: ubiquitous broadband, free email accounts, texting
- The cloud and outsourcing
- Mobile devices (smartphones)
- Emerging technologies (e.g., genetic screening)
- Civil disobedience in cyberspace
- Location services (e.g., Foursquare, Loopt and RFID transponders for toll kiosks and automated traffic volume display on billboards)
- Use of consumer-oriented devices or services in the workplace (e.g., iPads, Skype)
Changing and Conflicting Expectations by Individuals

- I expect:
  - To be able to do routine administrative tasks online (e.g., booking flights, paying bills, …) any time and from anywhere
  - The right people will have access to my personal information (e.g., my doctors, different services from the same campus)
  - That my confidential information will be properly used and protected and that I understand and have a say in what is “proper”
  - To be safe from on- and off-line threats/crimes

- Shaped by mainstream media, ubiquitous free net services, information fire hose, “Facebook culture,” blurring of work and personal lives
Research and Innovation

- **Technology research as human subjects research**
  - Using network traffic for research
- Openness – open exchange of information and ideas
- Does privacy stifle innovation? cf. EU Privacy Directive
In Loco Parentis

- Raising student awareness about the potential consequences of their actions
  - How to be smart about using Facebook, etc.
  - Illegal file sharing (DMCA / HEOA)
- Affirmatively protecting students
  - Making information about students available to credit card companies
  - Availability of information that could embarrass a student in the future
    - Publicly posting names in connection with police activity logs
    - Video of a heated classroom debate
Determining the Path Forward

Committee Deliverables: Recommendations
Foundational Questions
Statement of Community Principles and Values
Proposal for 2010
Committee Deliverables: Recommendations

- A framework
  - Statement of community principles and values
  - Governance
  - Accountability
  - Policies
- Sustainable review process
- Implementation process
Foundational Questions

1. How does the University balance the civil liberty of privacy with its many values and obligations?
2. Do we have a single policy for everyone, or different policies for different communities and/or types of data?
3. Is incidental personal use a right, a privilege or something else?
4. What is the University’s level of risk tolerance, especially for regulatory compliance?
5. How does the University determine appropriate ownership of, and access to, data by individuals, campuses, the administration, the Regents and external entities?
Statement of Community Principles and Values

- How does the University balance the civil liberty of privacy with its many values and obligations?

**SCENARIO: PRIVACY OF EMPLOYEE EMAIL**

- Supervisor cannot read employee’s email
- Supervisor can read only with employee’s consent
- Privacy protection only as required by law
- Supervisor obligated to read/review employee’s email

**MORE INDIVIDUAL PRIVACY**

Fosters:
- Freedom of inquiry and speech, academic freedom
- An ethical and respectful workplace
- High employee morale
- Ability to whistleblow confidentially

**LESS INDIVIDUAL PRIVACY**

Fosters:
- Better regulatory compliance
- Lower risk of privacy breaches
- Lower risk of financial, legal and reputational consequences
- Streamlining of business operations

DETERMINING THE PATH FORWARD
Proposal for 2010

- Working Group develops an initial draft statement of community principles and values
Logistics

Additional functional expertise?
Communications
Adjourn

universityofcalifornia.edu/privacyinitiative