A. Roadmap review (20 min)
   1. Summer Working Group activity (p.2)
   2. Today's agenda
   3. December 2nd in-person meeting at UCOP

B. The Electronic Communications Policy privacy stance (10 min, p.4)

C. Scenarios (50 min, p.7)
   1. Videotaping in the classroom for ADA purposes
   2. Web site tracking and analysis

D. Draft UC privacy principles (10 min, p.8)

Background material
   • Mining Student Data Could Save Lives
     The Chronicle of Higher Education, October 2, 2011
     chronicle.com/article/Mining-Student-Data-Could-Save/129231/

Gene Lucas, Executive Vice Chancellor, Santa Barbara (chair)
Robert Anderson, Chair, Systemwide Academic Senate
Christine Borgman, Professor of Information Studies, Los Angeles
Nathan Brostrom, Executive Vice President, UCOP
Karen Butter, University Librarian/Assistant Vice Chancellor, San Francisco
James Davis, Vice Provost, IT and Chief Academic Technology Officer, Los Angeles
David Ernst, AVP-IR&C and Chief Information Officer, UCOP
Matthew Franklin, Professor of Computer Science, Davis
Lee Giddings, Chief Compliance and Privacy Officer, San Diego Health Sciences
Brian Gresham, Assistant Director, Capital Planning and Space Management, Merced
Stephen Lau, Systemwide Policy Director for Information Management and Technology, UCOP
Harry LeGrande, Vice Chancellor for Student Affairs, Berkeley
Charles Louis, Vice Chancellor for Research, Riverside
John Meyer, Vice Chancellor, Administrative and Resource Management, Davis
Mike Minear, Chief Information Officer, Davis Health Services
Rafail Ostrovsky, Professor of Computer Science, Los Angeles
Lawrence Pitts, Provost and Executive Vice President, UCOP
Charles Robinson, Vice President and General Counsel, UCOP
Jessica Smith, UC Student Association (graduate), Berkeley
Peter Taylor, Chief Financial Officer, UCOP
Lynn Tierney, Associate Vice President, Communications, UCOP
Sheryl Vacca, SVP/Chief Compliance and Audit Officer, UCOP
Joshua Van Gelder, UC Student Association (undergraduate), Santa Cruz
Kent Wada, Director, Strategic IT and Privacy Policy, Los Angeles
Contents

Initiative Participants ........................................................................................................................................ 5

Executive Summary ........................................................................................................................................ 11

I Overview ..................................................................................................................................................... 13
   I.A Introduction ........................................................................................................................................ 15
   I.B Privacy and the University of California ............................................................................................ 18
   I.C Today’s Challenges ............................................................................................................................. 20
   I.D The Approach ..................................................................................................................................... 21
   I.E Structure of this Report ....................................................................................................................... 22

II Privacy and Information Security ................................................................................................................ 23

III Proposed Framework ................................................................................................................................... 43
   III.A Framework Elements ......................................................................................................................... 45
   III.B Statement of Privacy Values ............................................................................................................. 46
   III.C UC Privacy Principles ....................................................................................................................... 48
   III.D Statement of Information Security .................................................................................................. 50

IV Governance .................................................................................................................................................. 53
   IV.A Governance Model for Privacy and Information Security ............................................................... 55
   IV.B Toolkit: Privacy by Design .................................................................................................................. 56
   IV.C Toolkit: Privacy Balancing Test ........................................................................................................ 57
   IV.D Records and Information Management ............................................................................................ 63

V Strategic Directions for Policy ..................................................................................................................... 67
   V.A Turning Principles into Policy ............................................................................................................. 69
   V.B When University and Personal Data are Commingled .................................................................... 70
   V.C Use of Personal Electronic Devices by Individuals for University Business ...................................... 74

VI Scenarios ..................................................................................................................................................... 75

VII Conclusions ................................................................................................................................................ 77
   VII.A Recommended Actions ..................................................................................................................... 79
   VII.B Unresolved Issues ............................................................................................................................ 80

Appendices ....................................................................................................................................................... 81
   Appendix A. Steering Committee Charge .................................................................................................. 83
   Appendix B. Request to the UC Information Technology Policy and Security Committee ...................... 87
   Appendix C. Existing Systemwide Privacy-Related Policies ....................................................................... 88
   Appendix D. Report Process ...................................................................................................................... 90
   Appendix E. Sample Statement of UC Privacy Practices .......................................................................... 91
## Working Group

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Position Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Kent Wada, Los Angeles</td>
<td>Director, Strategic IT and Privacy Policy</td>
</tr>
<tr>
<td>UC Academic Senate Faculty Designate</td>
<td>David Steigmann, Berkeley</td>
<td>[September 2011–] Professor of Mechanical Engineering UC Academic Senate Committee on Academic Freedom</td>
</tr>
<tr>
<td>Information Technology Policy and IT Policy Manager</td>
<td>Karen Eft, Berkeley</td>
<td><img src="https://via.placeholder.com/150" alt="Image" /> [–April 2011] IT Policy Manager</td>
</tr>
<tr>
<td>Information Technology Security</td>
<td>Jon Good, Office of the President</td>
<td>Director, IT Security</td>
</tr>
<tr>
<td></td>
<td>Karl Heins, Santa Barbara</td>
<td>Chief Information Security Officer</td>
</tr>
<tr>
<td></td>
<td>Robert Ono, Davis</td>
<td>IT Security Coordinator</td>
</tr>
<tr>
<td>Campus Privacy</td>
<td>Ann Geyer, Berkeley</td>
<td>[May 2011–] Chief Privacy and Security Officer</td>
</tr>
<tr>
<td>Medical Center Privacy</td>
<td>Marti (Martha) Arvin, UCLA Health System</td>
<td>[June 2011–] Chief Compliance Officer</td>
</tr>
<tr>
<td></td>
<td>Kathleen Naughton, San Diego Health Sciences</td>
<td>Chief Privacy Officer</td>
</tr>
<tr>
<td>Systemwide Privacy Officer</td>
<td>Russell Opland, Office of the President</td>
<td>[–June 2011] Systemwide Privacy Officer and HIPAA Privacy and Security Officer</td>
</tr>
<tr>
<td>Legal Counsel</td>
<td>Maria Shanle, Office of the General Counsel</td>
<td>Senior University Counsel</td>
</tr>
<tr>
<td></td>
<td>Cynthia Vroom, Office of the General Counsel</td>
<td>[October 2011–] Senior University Counsel</td>
</tr>
<tr>
<td>Records Management Policies</td>
<td>Meta Clow, Santa Barbara</td>
<td>Policy and Information Stewardship Officer</td>
</tr>
</tbody>
</table>
IV. PRIVACY AND CONFIDENTIALITY

A. INTRODUCTION

The University recognizes that principles of academic freedom and shared governance, freedom of speech, and privacy hold important implications for the use of electronic communications. This Policy reflects these firmly-held principles within the context of the University’s legal and other obligations. The University respects the privacy of electronic communications in the same way that it respects the privacy of paper correspondence and telephone conversations, while seeking to ensure that University administrative records are accessible for the conduct of the University's business.

The University does not examine or disclose electronic communications records without the holder’s consent. Nonetheless, subject to the requirements for authorization, notification, and other conditions specified in this Policy, the University may examine or disclose electronic communications under very limited circumstances as described in Section IV.B, Access Without Consent.

University employees are prohibited from seeking out, using, or disclosing personal information in electronic communications without authorization (see Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information). University policy requires that its employees take necessary precautions to protect the confidentiality of personal information encountered either in the performance of their duties or otherwise (see Business and Finance Bulletin IS-3, Electronic Information Security).

University contracts with outside vendors for electronic communications services shall explicitly reflect and be consistent with this Policy and other University policies related to privacy.

B. ACCESS WITHOUT CONSENT

An electronic communications holder’s consent shall be obtained by the University prior to any access for the purpose of examination or disclosure of the contents of University electronic communications records in the holder’s possession, except as provided for below.

The University shall permit the examination or disclosure of electronic communications records without the consent of the holder of such records only: (i) when required by and consistent with law; (ii) when there is substantiated reason (as defined in Appendix A, Definitions) to believe that violations of law or of University policies listed in Appendix C, Policies Relating to Access Without
Consent, have taken place; (iii) when there are compelling circumstances as defined in Appendix A, Definitions; or (iv) under time-dependent, critical operational circumstances as defined in Appendix A, Definitions.

When under the circumstances described above the contents of electronic communications records must be examined or disclosed without the holder’s consent, the following shall apply:

1. **Authorization.** Except in emergency circumstances (as defined in Appendix A, Definitions) in accordance with Section IV.B.2, Emergency Circumstances, or except for subpoenas or search warrants in accordance with Section IV.B.6, Search Warrants and Subpoenas, such actions must be authorized in advance and in writing by the responsible campus Vice Chancellor or, for the Office of the President, the Senior Vice President, Business and Finance (see Section II.D, Responsibilities). This authority may not be further redelegated.

   Authorization shall be limited to the least perusal of contents and the least action necessary to resolve the situation.

2. **Emergency Circumstances.** In emergency circumstances as defined in Appendix A, Definitions, the least perusal of contents and the least action necessary to resolve the emergency may be taken immediately without authorization, but appropriate authorization must then be sought without delay following the procedures described in Section IV.B.1, Authorization, above.

3. **Notification.** The responsible authority or designee shall at the earliest opportunity that is lawful and consistent with other University policy notify the affected individual of the action(s) taken and the reasons for the action(s) taken.

   Each campus will issue in a manner consistent with law an annual report summarizing instances of authorized or emergency nonconsensual access pursuant to the provisions of this Section IV.B, Access Without Consent, without revealing personally identifiable data.

4. **Compliance with Law.** Actions taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances, shall be in full compliance with the law and other applicable University policies, including laws and policies listed in Appendix B, References. Advice of legal counsel must always be sought prior to any action involving electronic communications records (a)

---

1 On March 18, 2004 the Regents Committee on Audit approved changes to the Internal Audit Management Charter authorizing Internal Audit to have access to University information except where prohibited by law. [http://www.universityofcalifornia.edu/regents/regmeet/mar04.html]
stored on equipment not owned or housed by the University, or (b) whose content is protected under the federal Family Educational Rights and Privacy Act of 1974 (see Section IV.C.1.b, Student Information).

5. **Recourse.** Campus implementing procedures shall specify the process for review and appeal of actions taken under Sections IV.B.1, Authorization, and IV.B.2, Emergency Circumstances to provide a mechanism for recourse to individuals who believe that actions taken by employees or agents of the University were in violation of this Policy.

6. **Search Warrants and Subpoenas.** Search warrants and subpoenas are not subject to sections 1-2 and 4-5 above. Search warrants and subpoenas for electronic communications records shall be referred to University legal counsel at the Office of the General Counsel or designated officials at campus locations.

**Search Warrants.** Duly signed search warrants shall be processed in accordance with federal and state laws, University policies, and instructions in the warrant.

**Subpoenas.** Subpoenas shall be processed in accordance with applicable federal and state laws and University policies (see Business and Finance Bulletin RMP-10, Instructions for Responding to Subpoena). Campus officials shall provide advance notice to individuals whose records are the subject of a subpoena duces tecum in accordance with instructions and time requirements in RMP-10, section III.C, “Responding to requests for personal records of a consumer.”

C. **PRIVACY PROTECTIONS AND LIMITS**

1. **Privacy Protections**

   a. **Personal Information.** Federal and California law provide privacy protections for some information that personally identifies an individual. Business and Finance Bulletin RMP-8, Legal Requirements on Privacy of and Access to Information, provides guidelines for the collection and use of personal information in conformance with the law. These guidelines apply to information collected and disseminated by electronic means just as they do to records stored on paper and other media.

   b. **Student Information.** Users of electronic communications systems and services shall not disclose information about students in violation of the federal Family Educational Rights and Privacy Act of 1974 (FERPA), and the University policies that provide guidance in meeting FERPA requirements. See Business and Finance Bulletin RMP-8, Legal
Scenario #1
Recording Classrooms for Students with Disabilities

Background
Recording classroom discussions and lectures can be considered a reasonable accommodation for students with disabilities under the American with Disabilities Act, but it can have unintended direct and indirect privacy consequences for individuals in the classroom. People may modify their behavior when they know they are being recorded. They may feel uncomfortable or unwilling to talk about controversial subjects. In turn, this may alter the tenor of the discussion and alter the learning experience for others.

Scenario #2
Website Tracking and Analysis

Background
Tracking and analyzing website traffic to determine the effectiveness of website content and to customize content is a common industry practice. It can lower cost, unwanted content can be eliminated, and increase efficiency, individuals are presented with content customized to their interests without having to search for it.

Tracking, however, can easily violate an individual’s privacy since their behavior and actions are captured, stored and analyzed. Society as a whole is still grappling with how much tracking is too much and there has been proposed legislation to limit it.

Within UC, the Electronic Communications Policy generally prohibits tracking and analysis. There is a growing need and expectation for UC to provide customizable content. By prohibiting website tracking, we are potentially limiting UC’s ability to fill the needs of its community and placing the University at a competitive disadvantage. By allowing it though, we may be violating an individual’s privacy.
III.C UC Privacy Principles

Draft 5 – 10/10/2011

The University of California demonstrates its respect for the privacy of individuals by adopting and complying with the following Privacy Principles. These principles are derived from the UC Statement of Privacy Values and when used to guide the conduct and the decisions of all members of the University community, the mission of the University thrives and the community flourishes.

III.C.1 Autonomy Privacy Principles

III.C.1.a Free Inquiry

UC encourages free discourse without fear of reprisal or intimidation, subject to the privacy and safety of other individuals or University resources.

III.C.1.b Respect for Private Life

UC respects the privacy of individuals and actively encourages members of its community to esteem each other’s privacy and well-being.

III.C.1.c Surveillance

UC is guided by Fourth Amendment protections regarding surveillance of persons or places on campus, and balances the need for the safety of individuals and property with the individuals’ reasonable expectation of privacy in a particular location.

III.C.2 Information Privacy Principles

III.C.2.a Privacy by Design

The University builds privacy protections, which embody the principles stated below, into its business processes and information systems associated with the collection, use, disclosure, retention, or disposal of information about individuals. Business processes and information systems initiatives, revisions, or upgrades will be evaluated for their compliance with the UC privacy principles.

III.C.2.b Transparency and Notice

UC gives individuals advance notice of its information policies and practices for collecting, using, disclosing, retaining, and disposing of information about individuals.

UC collects, uses, discloses and retains only the minimum amount of information about individuals as necessary for the specified purpose and appropriately disposes of the information about individuals in accordance with its retention schedules.
Privacy notices clearly inform individuals about the purpose (how information will be used and the scope of information collected. [UC does not permit information about individuals collected for one purpose to be reused for another purpose unless the individual consents or the use is permitted or it’s required by law.] If UC suffers a breach which reasonably could adversely affect individuals or as required by law, the University provides notification individually or via its website or other channels of communication commensurate with the nature and scope of the violation.

III.C.2.c Choice
Prior to collecting, using, disclosing, or retaining information about individuals, UC provides individuals, whenever possible, with the ability to choose whether to and by what means to provide their information.

However, when the information about the individual is necessary to deliver a service or benefit or participate in an activity, the individual may be required to provide the information to receive the service or benefit or to participate.

III.C.2.d Information Review and Correction
Unless prohibited, UC provides individuals with 1) a way to review the information about themselves that they have provided and 2) a procedure to request the correction of inaccuracies.

III.C.2.e Information Protection
UC protects the information about individuals under its stewardship by providing appropriate employee training and by implementing privacy and security controls.

III.C.2.f Accountability
Every individual is accountable for complying with these principles and actively supporting UC’s commitment to respect the privacy of individuals.

Supervisors are responsible for providing information privacy training to those under their authority (employees, contractors, volunteers and others) who have access to information about individuals; and monitoring for and correcting gaps in actual practices.

UC investigates reported violations of information privacy principles and policies and, as appropriate, takes corrective measures.