Agenda for the December 3, 2010 videoconference (1-3pm)

A. Guest speaker: Chris Hoofnagle [p.10]

B. Privacy in the UC context [p.2]

C. A proposed structure for UC privacy [p.3]
   1. Draft UC privacy statement [p.4]
   2. Draft UC principles for safeguarding privacy, part I [p.5]

D. Applying the Generally Accepted Privacy Principles (GAPP) to a real-life scenario [p.8]

E. Background materials
   2. UC Statement of Ethical Values [p.11]
   3. UC Standards of Ethical Conduct [p.12]
   4. UC Diversity Statement [p.16]
   5. Steering Committee Members [p.17]
B. PRIVACY IN THE UC CONTEXT

The Problem Statement in the Steering Committee’s charge identified two types of privacy relevant to UC as an institution of higher education, cast by the Working Group as:

1. **Personal Privacy (the “civil liberty of privacy”):** Privacy of an individual’s actions (what people write, who they speak with, where they go, etc.).

2. **Information Privacy:**
   a. Privacy of confidential personal information (e.g., Social Security numbers, credit card numbers, patient records, student records).
   b. Privacy of information that may be personally identifiable (e.g., IP address).
   c. Privacy of confidential non-personal information (e.g., infrastructure plans, computer security configurations, intellectual property).

---

† The Working Group has not yet fully discussed issues relating to (1) personal privacy, (2b) the privacy of information that may be personally identifiable or (2c) the privacy of confidential non-personal information.

‡ Today’s agenda focuses mainly on (2a) the privacy of confidential personal information today.
C. A PROPOSED STRUCTURE FOR UC PRIVACY

UC has two existing examples – ethics and diversity – which offer a four-tier structural model that is proposed as a basis for privacy:

- **A statement** that asserts a value esteemed by UC. At this level, there is no prioritization or ranking and no intent to give guidance about resolving conflicts between values.
  - UC Statement of Ethical Values [p.11]
  - UC Diversity Statement [p.16]
  - UC Privacy Statement (draft) [p.4]

- **Principles** that express the value with more granular concepts, but still at a high level where no prioritization or ranking occurs.
  - Standards of Ethical Conduct [p.12]
  - Principles of Community
  - Principles for Safeguarding Privacy (draft) [p.5]

- **Policies** that explicate, with formal authority, how the institution operates: roles, responsibilities, operational goals and procedures.
  - Faculty code of conduct; Personnel policy manual; Whistleblower; Sexual harassment; Academic Personnel Policy; …
  - Personnel policy manual; Whistleblower; Sexual harassment; Academic Personnel Policy; …
  - ECP; IS; RMP; BUS-49; HIPAA; GLBA; Red Flags; Human subjects; Sexual harassment; Whistleblower; Personnel; …

- **Ongoing governance**
  - Office of Ethics, Compliance and Audit Services
  - UC AA/OO and Chief Diversity Officers Group
  - Adjudication process, group or guidelines

There are several areas where privacy principles overlap with the Standards of Ethical Conduct and the Principles of Community. Minimally, references between such related items will be made; in some cases, a proposal to revise an existing item may occur.
The University of California respects the privacy of the members of its community and of the individuals who entrust their personal information to the University. Privacy is an underpinning of academic freedom, upon which the mission of the University is dependent, and plays an important role in human dignity, essential for an ethical and respectful workplace.

The University must balance its respect for privacy with other values that it esteems and with its many legal, policy, and administrative obligations. Thus the University always strives for an appropriate balance between:

- 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.
C.2 DRAFT UC PRINCIPLES FOR SAFEGUARDING PRIVACY, PART I

The Problem Statement in the Steering Committee’s charge identified two types of privacy relevant to UC as an institution of higher education, cast by the Working Group as:

1. **Personal privacy**: Privacy of an individual’s actions (where people go, what they write, who they speak with, etc.)
2. **Information privacy**:
   a. Privacy of confidential personal information (e.g., Social Security numbers, credit card numbers, patient records, student records).
   b. Privacy of information that may be personally identifiable (e.g., IP address).
   c. Privacy of confidential non-personal information (e.g., infrastructure plans, computer security configurations, intellectual property).

While there are several models that speak to information privacy, the same is not so true of personal privacy.

**THE “UC PRINCIPLE”**
This “principle” speaks to the privacy of an individual’s actions, placing privacy in the context of the University as an institution of higher education.

At present, this section is only a placeholder. The Working Group has not fully discussed this type of privacy and does not yet know how this item may ultimately be expressed (i.e., it may not end up being a separate principle). However, it feels strongly that it be explicitly visible for future discussion.

**GAPP**
The Working Group has investigated existing models and has tentatively chosen the Generally Accepted Privacy Principles (GAPP) as a well-accepted exemplar to use as a working basis. GAPP was primarily developed for information privacy purposes; however, the principles are flexible enough to potentially cover personal privacy. The Working Group has discussed 2a most fully but needs further discussion of 2b and 2c.

A draft set of integrated principles for UC is expected for discussion at the next Steering Committee meeting.
THE “UC PRINCIPLE”
The following bullet points (a-e) are taken from the UC Electronic Communications Policy only to give a flavor for what the “UC Principle” is about. It has not yet been shaped into a more general principle or set of principles and is only provided as background at this time.

- **Limits on the monitoring of behavior.**
  a. 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.
  b. 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).
  c. University employees who operate and support electronic communications resources regularly monitor transmissions for the purpose of ensuring reliability and security of University electronic communications resources and services, and in that process might observe certain transactional information or the contents of electronic communications. Except as provided elsewhere in this Policy or by law, they are not permitted to seek out transactional information or contents when not germane to system operations and support, or to disclose or otherwise use what they have observed.
  d. In the process of such monitoring, any unavoidable examination of electronic communications (including transactional information) shall be limited to the least invasive degree of inspection required to perform such duties.
  e. Systems personnel shall not intentionally search the contents of electronic communications or transactional information for violations of law or policy.

**GENERALLY ACCEPTED PRIVACY PRINCIPLES**
The following are the ten Generally Accepted Privacy Principles:

1. **Management.** The entity defines, documents, communicates and assigns accountability for its privacy policies and procedures.
2. **Notice.** The entity provides notice about its privacy policies and procedures and identifies the purposes for which personal information is collected, used, retained and disclosed.
3. **Choice and consent.** The entity describes the choices available to the individual and obtains implicit or explicit consent with respect to the collection, use and disclosure of personal information.
4. **Collection.** The entity collects personal information only for the purposes identified in the notice.
5. **Use, retention and disposal.** The entity limits the use of personal information to the purposes identified in the notice and for which the individual has provided implicit or explicit consent. The entity retains personal information for only as long as necessary to
fulfill the stated purposes or as required by law or regulation and thereafter appropriately disposes of such information.

6. **Access.** The entity provides individuals with access to their personal information for review and update.

7. **Disclosure to third parties.** The entity discloses personal information to third parties only for the purposes identified in the notice and with the implicit or explicit consent of the individual.

8. **Security for privacy.** The entity protects personal information against unauthorized access (both physical and logical).

9. **Quality.** The entity maintains accurate, complete and relevant personal information for the purposes identified in the notice.

10. **Monitoring and enforcement.** The entity monitors compliance with its privacy policies and procedures and has procedures to address privacy-related complaints and disputes.

These definitions are at an executive summary level, with considerable detail behind them.
D. APPLYING GAPP TO A REAL-LIFE SCENARIO

Scenario: Use of a third party provider for UC health information as part of a research project.

1. **Management.** Review of the third party contract in the light of UC privacy policies, procedures and risk acceptance level and addressing any identified privacy risks. Identifying any needed changes to policies and procedures.

2. **Notice.** A notice that details privacy implications is provided to participants so that they can make an informed decision. For example, a click through notice, annual email notices, etc.

3. **Choice and consent.** Any choices that are available to the user are clearly identified, for example any options to not participate in the project or selectively withhold information (i.e. anonymous). If consent is required, processes and procedures are in place to gain consent prior to information collection.

4. **Collection.** The contract with the third party provider explicitly states what will be sent to the third party and for what purpose. The minimal data required is used by the research project. The participants are told what personal information will be collected, who will be collecting it and why.

5. **Use, retention and disposal.** The third party contract addresses retention schedules, disposal of data and how the data is being used by the third party. In this case, the retention schedule and disposal of data may be based upon UC policies. This information is also provided to the participants.

6. **Access.** A process is made available for participants to inspect and correct data that is incorrect. The correction may be done by UC or by the participant. A process is also in place for participants to notify UC of any incorrect data.

7. **Disclosure to third parties.** The contract addresses any data reuse and disclosure to any secondary third parties by the primary third party. Information on any third parties is made available to the participant.

8. **Security for privacy.** Security provided by the third party is addressed, as well as requirements for notifying UC in the event of breaches of data. A review is made by UC to ensure the security of the research project information.

9. **Quality.** The research project has a component that addresses data quality so that any data corruption is identified as quickly as possible and corrected.

10. **Monitoring and enforcement.** UC checks to see if processes are in place in accordance with UC policies. For example, if there is a process for participants to identify incorrect data or to perform reviews of third party contracts.
Chris Hoofnagle
Lecturer in Residence, Director – Information Privacy Programs
510-643-0213, choofnagle@law.berkeley.edu

Chris Jay Hoofnagle is director of the Berkeley Center for Law & Technology’s information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic. He is an expert in information privacy law.

Hoofnagle’s recent work focuses on promoting competition among financial institutions to prevent identity theft. In Identity Theft: Making the Unknown Knowns Known, he discusses the problem of “synthetic identity theft,” a form of crime where an impostor fabricates personal information and yet still can obtain credit accounts. Hoofnagle argues that the rise of this form of fraud demonstrates a fundamental failure in banks’ anti-fraud gatekeeper function, and proposes market reforms for reducing identity theft.

With Jennifer King, Hoofnagle has started a consumer privacy survey research project. This project explores consumers’ understanding of privacy and tests notions of consumer autonomy underlying existing self-regulatory privacy rules.

Hoofnagle has long called attention to the civil liberties risks posed by private-sector database companies. In Big Brother’s Little Helpers, he argued that civil libertarians’ focus on government behavior left private-sector firms free to create the very “federal data center” that the Privacy Act of 1974 was enacted to prevent. These ideas were presented in the Emmy award winning documentary, Big Brother, Big Business. After commercial database companies suffered security breaches, he articulated a framework for regulating the industry in A Model Regime of Privacy, with George Washington Law School Professor Daniel J. Solove.

Prior to joining Berkeley Law, Hoofnagle was a non-residential fellow with Stanford Law School’s Center for Internet and Society. Prior to that, Hoofnagle focused on regulation of telemarketing, financial services privacy, and credit reporting at the Electronic Privacy Information Center in Washington, DC. He was the author of an amicus brief in Remsburg v. Docusearch, a case in which the Supreme Court of New Hampshire held that private investigators have a duty to exercise reasonable care towards individuals being investigated, and that individuals may bring common law privacy claims against investigators who acquire personal information through pretexting. He also authored an amicus brief in Kehoe v. Fidelity Federal Bank and Trust, in which the 11th Circuit held that individuals do not need to demonstrate harm to collect monetary damages from invasions of privacy. The decision makes it economically viable for individuals to vindicate privacy rights in court, and resulted in a $50 million settlement including direct payments to thousands of affected plaintiffs.

Hoofnagle co-chairs the annual Privacy Law Scholars Conference. He is licensed to practice in California and Washington, DC.

Education:
B.A., University of Georgia (1996)
J.D., University of Georgia School of Law (2000)
E.2 UC STATEMENT OF ETHICAL VALUES

http://www.ucop.edu/ucophome/coordrev/policy/Stmt_Stds_Ethics.pdf

Members of the University of California community are committed to the highest ethical standards in furtherance of our mission of teaching, research and public service. We recognize that we hold the University in trust for the people of the State of California. Our policies, procedures, and standards provide guidance for application of the ethical values stated below in our daily life and work as members of this community.

We are committed to:

* **Integrity**
  We will conduct ourselves with integrity in our dealings with and on behalf of the University.

* **Excellence**
  We will conscientiously strive for excellence in our work.

* **Accountability**
  We will be accountable as individuals and as members of this community for our ethical conduct and for compliance with applicable laws and University policies and directives.

* **Respect**
  We will respect the rights and dignity of others.
E.3 UC STANDARDS OF ETHICAL CONDUCT
http://www.universityofcalifornia.edu/compaudit/ethicalconduct.html

Purpose
Pursuit of the University of California mission of teaching, research and public service requires a shared commitment to the core values of the University as well as a commitment to the ethical conduct of all University activities. In that spirit, the Standards of Ethical Conduct are a statement of our belief in ethical, legal and professional behavior in all of our dealings inside and outside the University.

Applicability
The Standards of Ethical Conduct apply to all members of the University community, including The Regents, Officers of The Regents, faculty and other academic personnel, staff, students, volunteers, contractors, agents and others associated with the University. Organizationally, the Standards apply to campuses, the National Laboratories, the Office of the President, the Division of Agriculture and Natural Resources, campus organizations, foundations, alumni associations and support groups.

1. Fair Dealing
Members of the University community are expected to conduct themselves ethically, honestly and with integrity in all dealings. This means principles of fairness, good faith and respect consistent with laws, regulations and University policies govern our conduct with others both inside and outside the community. Each situation needs to be examined in accordance with the Standards of Ethical Conduct. No unlawful practice or a practice at odds with these standards can be justified on the basis of customary practice, expediency, or achieving a “higher” purpose.

2. Individual Responsibility and Accountability
Members of the University community are expected to exercise responsibility appropriate to their position and delegated authorities. They are responsible to each other, the University and the University’s stakeholders both for their actions and their decisions not to act. Each individual is expected to conduct the business of the University in accordance with the Core Values and the Standards of Ethical Conduct, exercising sound judgment and serving the best interests of the institution and the community.

3. Respect for Others
The University is committed to the principle of treating each community member with respect and dignity. The University prohibits discrimination and harassment and provides equal opportunities for all community members and applicants regarding less of race, color, national origin, religion, sex, gender identity, pregnancy, physical or mental disability, medical condition (cancer-related or genetic characteristics), ancestry, marital status, age, sexual orientation, citizenship, or status as a covered veteran. Further, romantic or sexual relationships between faculty responsible for academic supervision, evaluation or instruction and their students are prohibited. The University is committed to creating a safe and drug free workplace. Following is a list of the principal policies and reference materials available in support of this standard:

- The Faculty Code of Conduct
- Academic Personnel Policy Manual
- The Faculty Handbook
- Personnel Policies for Staff Members
- Policies Applying to Campus Activities, Organizations and Students
- Policy on Sexual Harassment and Procedures for Responding to Reports of Sexual Harassment
University policies on nondiscrimination and affirmative action
Campus, laboratory and Office of the President Principles of Community

The University's health sciences enterprises are committed to the ethical and compassionate treatment of patients and have established policies and statements of patient rights in support of this principle.

4. Compliance with Applicable Laws and Regulations
Institutions of higher education are subject to many of the same laws and regulations as other enterprises, as well as those particular to public entities. There are also additional requirements unique to higher education. Members of the University community are expected to become familiar with the laws and regulations bearing on their areas of responsibility. Many but not all legal requirements are embodied in University policies. Failure to comply can have serious adverse consequences both for individuals and for the University, in terms of reputation, finances and the health and safety of the community. University business is to be conducted in conformance with legal requirements, including contractual commitments undertaken by individuals authorized to bind the University to such commitments.

The Office of the General Counsel has responsibility for interpretation of legal requirements.

5. Compliance with Applicable University Policies, Procedures and Other Forms of Guidance
University policies and procedures are designed to inform our everyday responsibilities, to set minimum standards and to give University community members notice of expectations. Members of the University community are expected to transact all University business in conformance with policies and procedures and accordingly have an obligation to become familiar with those that bear on their areas of responsibility. Each member is expected to seek clarification on a policy or other University directive he or she finds to be unclear, outdated or at odds with University objectives. It is not acceptable to ignore or disobey policies if one is not in agreement with them, or to avoid compliance by deliberately seeking loopholes.

In some cases, University employees are also governed by ethical codes or standards of their professions or disciplines—some examples are attorneys, auditors, physicians and counseling staff. It is expected that those employees will comply with applicable professional standards in addition to laws and regulations.

6. Conflicts of Interest or Commitment
Employee members of the University community are expected to devote primary professional allegiance to the University and to the mission of teaching, research and public service. Outside employment must not interfere with University duties. Outside professional activities, personal financial interests, or acceptance of benefits from third parties can create actual or perceived conflicts between the University's mission and an individual's private interests. University community members who have certain professional or financial interests are expected to disclose them in compliance with applicable conflict of interest/conflict of commitment policies. In all matters, community members are expected to take appropriate steps, including consultation if issues are unclear, to avoid both conflicts of interest and the appearance of such conflicts.

7. Ethical Conduct of Research
All members of the University community engaged in research are expected to conduct their research with integrity and intellectual honesty at all times and with appropriate regard for human and animal subjects. To protect the rights of human subjects, all research involving human subjects is to be
reviewed by institutional review boards. Similarly, to protect the welfare of animal subjects, all research involving animal subjects is to be reviewed by institutional animal care and use committees. The University prohibits research misconduct. Members of the University community engaged in research are not to: fabricate data or results; change or knowingly omit data or results to misrepresent results in the research record; or intentionally misappropriate the ideas, writings, research, or findings of others. All those engaged in research are expected to pursue the advancement of knowledge while meeting the highest standards of honesty, accuracy, and objectivity. They are also expected to demonstrate accountability for sponsors’ funds and to comply with specific terms and conditions of contracts and grants.

8. Records: Confidentiality/Privacy and Access
The University is the custodian of many types of information, including that which is confidential, proprietary and private. Individuals who have access to such information are expected to be familiar and to comply with applicable laws, University policies, directives and agreements pertaining to access, use, protection and disclosure of such information. Computer security and privacy are also subject to law and University policy.

Information on the University’s principles of privacy or on specific privacy laws may be obtained from the respective campus or laboratory information privacy office.

The public right to information access and the individual’s right to privacy are both governed by state and federal law, as well as by University policies and procedures. The legal provisions and the policies are based upon the principle that access to information concerning the conduct of the people’s business is a fundamental and necessary right of every person, as is the right of individuals to privacy.

9. Internal Controls
Internal controls are the processes employed to help ensure that the University’s business is carried out in accordance with these Standards, University policies and procedures, applicable laws and regulations and sound business practices. They help to promote efficient operations, accurate financial reporting, protection of assets and responsible fiscal management. All members of the University community are responsible for internal controls. Each business unit or department head is specifically responsible for ensuring that internal controls are established, properly documented and maintained for activities within their jurisdiction. Any individual entrusted with funds, including principal investigators, is responsible for ensuring that adequate internal controls exist over the use and accountability of such funds. The University has adopted the principles of internal controls published by the Committee of Sponsoring Organizations (COSO) of the Treadway Commission.

10. Use of University Resources
University resources may only be used for activities on behalf of the University. They may not be used for private gain or personal purposes except in limited circumstances permitted by existing policy where incidental personal use does not conflict with and is reasonable in relation to University duties (e.g. telephones). Members of the University community are expected to treat University property with care and to adhere to laws, policies and procedures for the acquisition, use, maintenance, record keeping and disposal of University property. For purposes of applying this policy, University resources is defined to include but not be limited to the following, whether owned by or under the management of the University (for example, property of the federal government at the National Laboratories):

- Cash, and other assets whether tangible or intangible; real or personal property;
- Receivables and other rights or claims against third parties;
- Intellectual property rights;
- Effort of University personnel and of any non-University entity billing the University for effort;
Facilities and the rights to use University facilities;
- The University’s name;
- University records, including student and patient records; and
- The University information technology infrastructure.

11. Financial Reporting
All University accounting and financial records, tax reports, expense reports, time sheets and effort reports, and other documents including those submitted to government agencies must be accurate, clear and complete. All published financial reports will make full, fair, accurate, timely and understandable disclosures as required under generally accepted accounting principles for government entities, bond covenant agreements and other requirements. Certain individuals with responsibility for the preparation of financial statements and disclosures, or elements thereof, may be required to make attestations in support of the Standards.

12. Reporting Violations and Protection from Retaliation
Members of the University community are strongly encouraged to report all known or suspected improper governmental activities (IGAs) under the provisions of the Policy on Reporting and Investigating Allegations of Suspected Improper Governmental Activities (Whistleblower Policy). Managers and persons in supervisory roles are required to report allegations presented to them and to report suspected IGAs that come to their attention in the ordinary course of performing their supervisory duties. Reporting parties, including managers and supervisors, will be protected from retaliation for making such a report under the Policy for Protection of Whistleblowers from Retaliation and Guidelines for Reviewing Retaliation Complaints (Whistleblower Retaliation Policy).

Adopted by The Regents of the University of California, May, 2005.
E.4 UC DIVERSITY STATEMENT
http://www.universityofcalifornia.edu/diversity/diversity.html

Adopted by the Assembly of the Academic Senate May 10, 2006
Endorsed by the President of the University of California June 30, 2006
Adopted by the Regents of the University of California, September 19, 2007

The diversity of the people of California has been the source of innovative ideas and creative accomplishments throughout the state's history into the present. Diversity – a defining feature of California's past, present, and future – refers to the variety of personal experiences, values, and worldviews that arise from differences of culture and circumstance. Such differences include race, ethnicity, gender, age, religion, language, abilities/disabilities, sexual orientation, socioeconomic status, and geographic region, and more.

Because the core mission of the University of California is to serve the interests of the State of California, it must seek to achieve diversity among its student bodies and among its employees. The State of California has a compelling interest in making sure that people from all backgrounds perceive that access to the University is possible for talented students, staff, and faculty from all groups. The knowledge that the University of California is open to qualified students from all groups, and thus serves all parts of the community equitably, helps sustain the social fabric of the State.

Diversity should also be integral to the University's achievement of excellence. Diversity can enhance the ability of the University to accomplish its academic mission. Diversity aims to broaden and deepen both the educational experience and the scholarly environment, as students and faculty learn to interact effectively with each other, preparing them to participate in an increasingly complex and pluralistic society. Ideas, and practices based on those ideas, can be made richer by the process of being born and nurtured in a diverse community. The pluralistic university can model a process of proposing and testing ideas through respectful, civil communication. Educational excellence that truly incorporates diversity thus can promote mutual respect and make possible the full, effective use of the talents and abilities of all to foster innovation and train future leadership.

Therefore, the University of California renews its commitment to the full realization of its historic promise to recognize and nurture merit, talent, and achievement by supporting diversity and equal opportunity in its education, services, and administration, as well as research and creative activity. The University particularly acknowledges the acute need to remove barriers to the recruitment, retention, and advancement of talented students, faculty, and staff from historically excluded populations who are currently underrepresented.
## E.5 STEERING COMMITTEE MEMBERS

<table>
<thead>
<tr>
<th>Role</th>
<th>Name</th>
<th>Affiliation</th>
</tr>
</thead>
<tbody>
<tr>
<td>Chair</td>
<td>Gene Lucas</td>
<td>Santa Barbara</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Executive Vice Chancellor</td>
</tr>
<tr>
<td>Systemwide Representation and Support</td>
<td>Sheryl Vacca</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Senior Vice President, Chief Compliance and Audit Officer</td>
</tr>
<tr>
<td></td>
<td>David Ernst</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associate Vice President, Information Resources and Communications and Chief Information Officer</td>
</tr>
<tr>
<td>Academic Senate:</td>
<td>Matthew Franklin</td>
<td>Davis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Professor of Computer Science</td>
</tr>
<tr>
<td></td>
<td>Rafail Ostrovsky</td>
<td>Los Angeles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Professor of Computer Science</td>
</tr>
<tr>
<td></td>
<td>TBA</td>
<td></td>
</tr>
<tr>
<td>Vice Chancellor for Research</td>
<td>Charles Louis</td>
<td>Riverside</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vice Chancellor</td>
</tr>
<tr>
<td>Vice Chancellor for Administration</td>
<td>John Meyer</td>
<td>Davis</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vice Chancellor, Administrative and Resource Management</td>
</tr>
<tr>
<td>Vice Chancellor for Student Affairs</td>
<td>Harry LeGrande</td>
<td>Berkeley</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vice Chancellor</td>
</tr>
<tr>
<td>Campus IT Representative</td>
<td>James Davis</td>
<td>Los Angeles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vice Provost, IT and Chief Academic Technology Officer</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chair, UCLA Privacy Board</td>
</tr>
<tr>
<td>Medical Center CIO</td>
<td>Mike Minear</td>
<td>Davis Health Services</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chief Information Officer</td>
</tr>
<tr>
<td>University Librarian</td>
<td>Karen Butter</td>
<td>San Francisco</td>
</tr>
<tr>
<td></td>
<td></td>
<td>University Librarian/Assistant Vice Chancellor</td>
</tr>
<tr>
<td>Medical Center Privacy Officer</td>
<td>Lee Giddings</td>
<td>San Diego Health Sciences</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chief Compliance and Privacy Officer</td>
</tr>
<tr>
<td>General Counsel</td>
<td>Charlie Robinson</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Vice President and General Counsel</td>
</tr>
<tr>
<td>Chair, Academic Senate</td>
<td>Dan Simmons</td>
<td>Systemwide Academic Senate</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Academic Senate Chair</td>
</tr>
<tr>
<td>UCOP Academic Affairs</td>
<td>Lawrence Pitts</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Provost and Executive Vice President</td>
</tr>
<tr>
<td>UCOP Business Operations</td>
<td>Nathan Brostrom</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Executive Vice President</td>
</tr>
<tr>
<td>President’s Compliance Committee</td>
<td>Peter Taylor</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Chief Financial Officer</td>
</tr>
<tr>
<td>Communications</td>
<td>Lynn Tierney</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Associate Vice President</td>
</tr>
<tr>
<td>Systemwide Policy Director for</td>
<td>Stephen Lau</td>
<td>Office of the President</td>
</tr>
<tr>
<td>Information Management and Technology</td>
<td></td>
<td>Systemwide Policy Director</td>
</tr>
<tr>
<td>Systemwide Privacy Officer</td>
<td>Russ Opland</td>
<td>Office of the President</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Systemwide Privacy Officer and HIPAA Privacy and Security Officer</td>
</tr>
<tr>
<td>UC Undergraduate Student</td>
<td>Olutwatobi Afolayan</td>
<td>Riverside</td>
</tr>
<tr>
<td></td>
<td></td>
<td>UC Student Association</td>
</tr>
<tr>
<td>UC Graduate Student</td>
<td>TBD</td>
<td>UC Student Association</td>
</tr>
<tr>
<td>Council of University of California</td>
<td>Brian Gresham</td>
<td>Merced</td>
</tr>
<tr>
<td>Staff Assemblies</td>
<td></td>
<td>Chair Elect, CUCSA</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Assistant Director, Capital Planning and Space Management</td>
</tr>
<tr>
<td>Working Group Chair</td>
<td>Kent Wada</td>
<td>Los Angeles</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Director, Strategic IT and Privacy Policy</td>
</tr>
</tbody>
</table>