



Office of the Executive Vice Chancellor  
Santa Barbara, California 93106-2035  
Telephone: (805) 893-2126  
Facsimile: (805) 893-7712

February 28, 2013

Mark Yudof  
President  
University of California  
1111 Franklin Street  
Oakland, CA 94607

Dear President Yudof:

I am pleased to provide you with the attached recommendations on behalf of the University of California Privacy and Information Security Steering Committee. These recommendations respond to your charge to the Committee to perform a comprehensive review of the University's current privacy and information security policy framework and to make recommendations about how the University should address related near-term policy issues and longer-term governance issues. Specifically:

- An overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;
- Governance, implementation, and accountability structures across the University with respect to privacy and information security;
- 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; and
- Specific actions or phases needed to implement the proposed framework as University policy.

The recommendations distill an expansive and nuanced examination of privacy frameworks employed in this country and internationally, of privacy models in use at other institutions as well as those articulated by leading privacy scholars, of the UC environment with respect to privacy, and of the meaning of privacy itself. The Committee was guided by the following principles in considering this charge and in framing its recommendations:

- We must maximally enable the mission of the University by supporting the values of academic and intellectual freedom.
- We must be good stewards of the information entrusted to the University.
- We must ensure that the University has access to information resources for legitimate business purposes.
- We must have a University community with clear expectations of privacy—both privileges and obligations of individuals and of the institution.
- We must make decisions within an institutional context.

February 28, 2013

Page 2

- We must acknowledge the distributed nature of information stewardship at UC, where responsibility for privacy and information security resides at every level.

A primary goal of this report is to propose an integrated approach to privacy and information security. However, information security programs have greater maturity within the University. The apparent greater focus on privacy in this report is reflective of the relative states of privacy and of information security at UC at present.

A tremendous amount of time and effort was given by the Steering Committee and by the Working Group charged to support the Committee's efforts by framing key issues and options for discussion and turning those deliberations into concrete form. Several members were key to shaping the final outcome of these recommendations.

The Steering Committee and Working Group believe that the holistic approach established by the report's recommendations is unique across higher education ... and beyond. We believe that the approach drives toward a unified privacy model that is led by the University's mission and values and against which existing guidance for decision-making, policy, and practice in the area of privacy at the University of California can and should be aligned over time. We hope you will agree.

Sheryl Vacca and I would like to offer to walk you through this report, which we feel will be helpful in determining next steps for vetting and adopting the proposals in this report. Of course, if you have any questions or would like to discuss any aspect of the report immediately, please let me know.

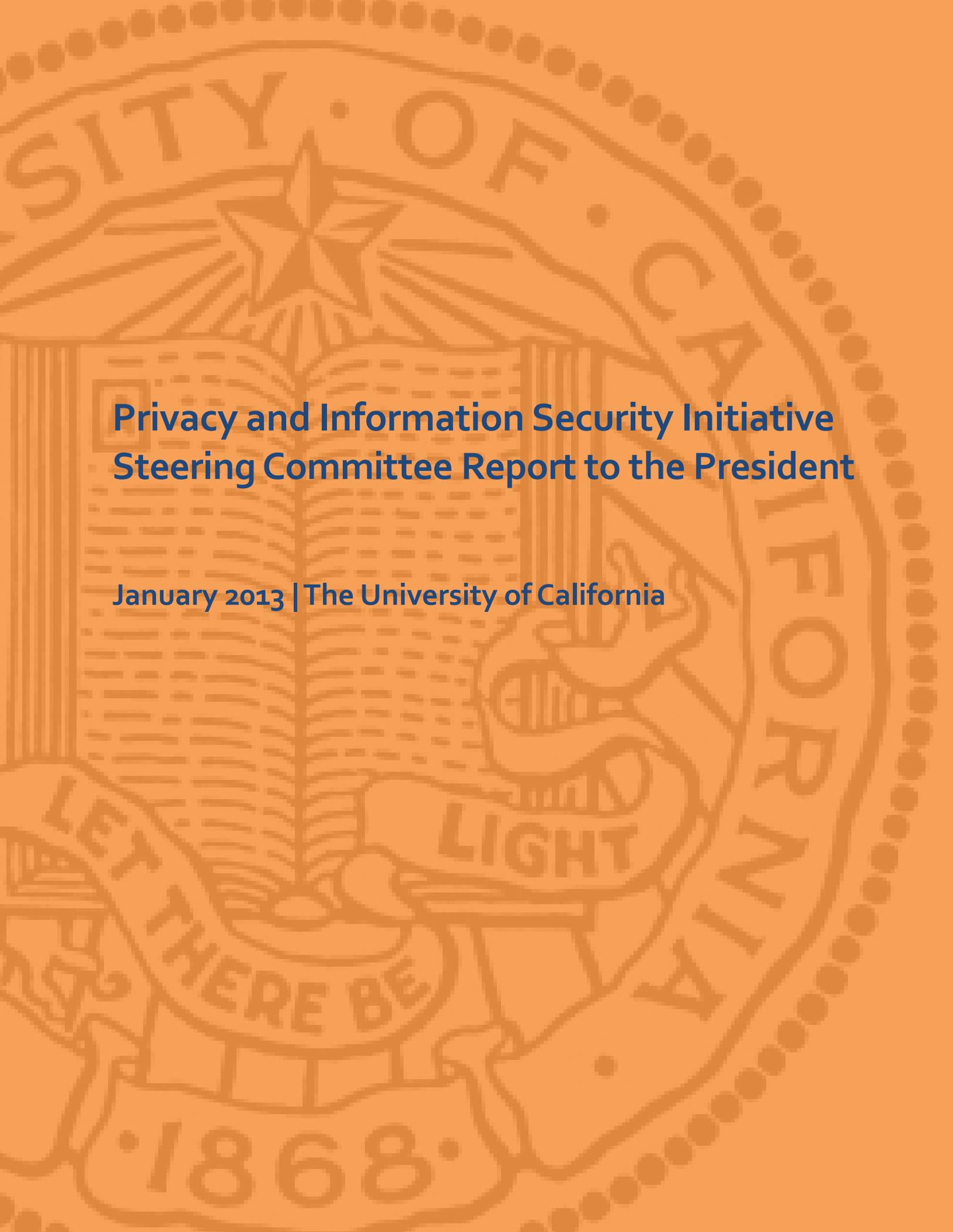
Sincerely,



Gene Lucas  
Steering Committee Chair  
President's Initiative on Privacy and Information Security

encl: Steering Committee Report to the President

cc: Steering Committee members  
Working Group members  
Chief of Staff Robinson

The background of the page is a large, light orange seal of the University of California. The seal features a central figure holding a book and a torch, with the motto "LET THERE BE LIGHT" on a banner. The words "UNIVERSITY OF CALIFORNIA" are written around the perimeter, and the year "1868" is at the bottom.

# Privacy and Information Security Initiative Steering Committee Report to the President

January 2013 | The University of California

## Contents

<b>Executive Summary .....</b>	<b>1</b>
<b>I Introduction .....</b>	<b>6</b>
Background.....	7
Approach and Deliverables of the Steering Committee.....	8
Defining Privacy and Information Security.....	9
Observations.....	11
<b>II Recommendations.....</b>	<b>12</b>
UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process.....	13
Campus Privacy and Information Security Boards.....	20
Systemwide Board for Privacy and Information Security .....	21
Campus Privacy Official.....	22
<b>III Proposed Implementation Schedule .....</b>	<b>23</b>
<b>Appendices.....</b>	<b>26</b>
Appendix A. Steering Committee Charge .....	27
Appendix B. UC Chief Information Security and Privacy Officer.....	30
Appendix C. Existing Systemwide Policies Related to Privacy and Information Security.....	31
Appendix D. Existing Campus Privacy and/or Information Security Committees.....	33
<b>Initiative Participants .....</b>	<b>38</b>
<b>Glossary .....</b>	<b>43</b>

---

# EXECUTIVE SUMMARY

---

## Privacy, Information Security, and the University of California

Privacy is fundamental to the University. It plays an important role in upholding human dignity and in sustaining a strong and vibrant society. Respecting privacy is an essential part of what it means to be a good citizen, whether as an individual or as an institution. Ensuring such privacy is one of the many values and obligations of the University of California.

Academic and intellectual freedoms 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 living out these values possible.

Privacy is also a basis for an ethical and respectful workplace.

Privacy, together with information security, underpins the University's ability to be a good steward of the information entrusted to it by its 235,000 students and 185,000 employees, and by its extended community of patients, alumni, donors, volunteers and many others; and obligations in both areas continue to proliferate even as the transparency required of public institutions remains an important cornerstone of the University.

How privacy is balanced against the many rights, values, and desires of our society is among the most challenging issues of our time.

### The Charge

In June of 2010, UC President Mark Yudof convened the University of California Privacy and Information Security Steering Committee to perform a comprehensive review of the University's current privacy and information security policy framework and to make recommendations about how the University should address near-term policy issues and longer-term governance issues. The specific charge to the Committee was to make recommendations for:

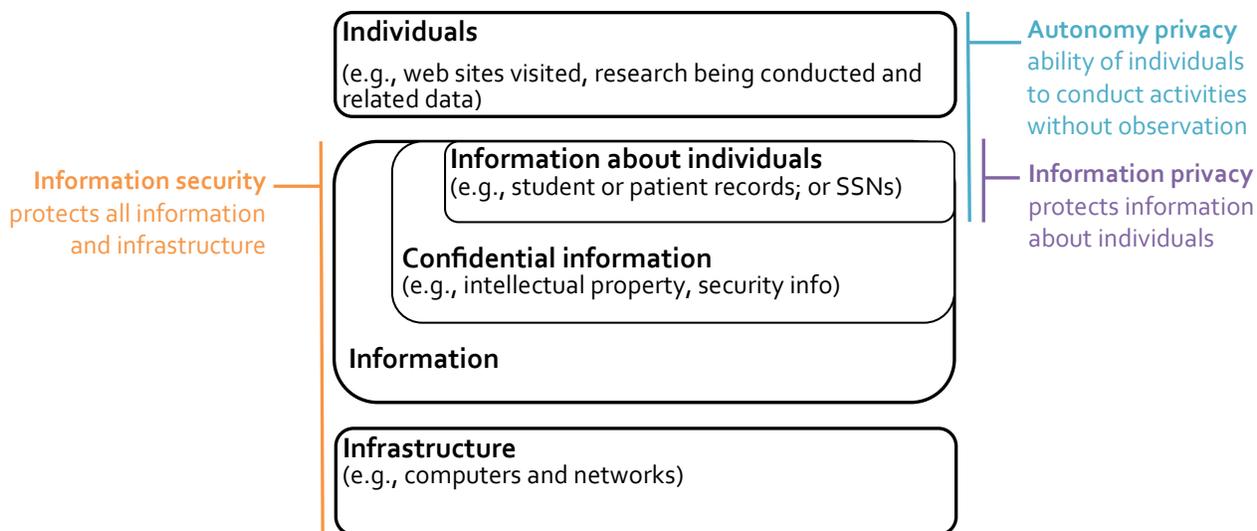
- |  |   |
|--|---|
| 1. An overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;   | All recommendations and Definitions (page 9)  |
| 2. Governance, implementation, and accountability structures across the University with respect to privacy and information security;   | Recommendations 2, 3, and 4                   |
| 3. 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; and | All recommendations                           |
| 4. Specific actions or phases needed to implement the proposed framework as University policy.   | Section III, Proposed Implementation Schedule |

### Approach and Deliverables

In examining the issues of privacy and information security in today's world and in the context of the constellation of values and obligations of the University of California, the Steering Committee reviewed relevant core concepts and principles and consulted with constituents and experts. In addition to President Yudof's charge, the committee developed a series of principles that guided its work.

One of the Committee’s early challenges was to distinguish the intertwined concepts of *autonomy privacy*, *information privacy*, and *information security* from one another, name them and define them:

- *Autonomy privacy* is an individual’s ability to conduct activities without concern of or actual observation.
- *Information privacy* is the appropriate protection, use, and dissemination of information about individuals.
- *Information security* is the protection of information resources from unauthorized access, which could compromise their confidentiality, integrity, and availability.



The University’s long experience with privacy, when viewed through the lens of these new definitions, reveals gaps, silos, and challenges in its approach to addressing privacy. An integrated view is required across autonomy privacy, information privacy, and information security; across the University’s operating model of distributing stewardship and accountability; and across individual expectations that typically evolve from a different viewpoint than do University policies and at a different pace than do technology and social norms. The recommendations in this report speak to strategic action; but a key component for addressing operational integration was put in place in March 2012 with the hiring of a new Systemwide position, the UC Chief Information Security and Privacy Officer (see Appendix B).

A primary goal of this report is to propose an integrated approach to privacy and information security. However, information security programs have greater maturity within the University. For example, whereas existing UC policy already requires the designation of an information security officer and implementation of an information security program, there is no equivalent for privacy. The apparent greater focus on privacy in this report is reflective of the relative states of privacy and of information security at UC at present.

The Committee entered this initiative with an expected focus on UC’s privacy policies. It emerged with a more holistic, integrated view of privacy. The recommendations presented here, therefore, not only are responsive to the President’s charge; but also drive toward a unified privacy model, led by the University’s mission and values, against which existing guidance for decision-making, policy, and practice in the area of privacy at the University of California can and should be aligned over time.

## Recommendations

Ultimately, the Steering Committee arrived at four recommendations it believes define an overarching privacy framework that will pave the way for an integrated approach to privacy and information security for the University of California.

**RECOMMENDATION 1: UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process.** The University shall formally adopt the proposed UC Statement of Privacy Values, Privacy Principles, and Privacy Balancing Process.

The **UC Privacy Values, Principles, and Balancing Process** are foundational elements integral to any privacy program. By explicitly articulating these elements outside the boundaries of any specific policy, functional area, or regulation, the intent is to create a unifying set of privacy expectations across the entire University community and provide a basis for achieving a common approach to privacy-related decisions – yet allow the flexibility that recognizes the University as a vast, complex organization with significantly varying needs and obligations that will change over time. This approach parallels the model of the UC Statement of Ethical Values and Standards of Ethical Conduct.

1. The **UC Statement of Privacy Values** declares privacy – of both autonomy and information – as an important value of the University, as this is not explicitly done elsewhere; and clarifies that privacy is one of many values and obligations of the University.
2. The **UC Privacy Principles** define a set of privacy principles for the University that are derived from, and give concrete guidance about, the Statement of Privacy Values.
3. The **Privacy Balancing Process** provides a mechanism for adjudicating between competing values, obligations, and interests, whether as a tool in making policy or to guide decision-making in specific situations, and even in a changing context.

**RECOMMENDATION 2: Campus Privacy and Information Security Boards.** Each Chancellor shall form a joint Academic Senate–Administration board to advise him or her, or a designee, on privacy and information security; set strategic direction for autonomy privacy, information privacy, and information security; champion the UC Privacy Values, Principles, and Balancing Process; and monitor compliance and assess risk and effectiveness of campus privacy and information security programs.

**RECOMMENDATION 3: Systemwide Board for Privacy and Information Security.** The President shall form a joint Academic Senate–Administration board systemwide to advise him or her, or a designee, on privacy and information security; set strategic direction for autonomy privacy, information privacy, and information security; steward the UC Privacy Values, Principles, and Balancing Process; and monitor their effective implementation by campus privacy and information security boards.

Privacy and information security governance responsibilities need to exist at both the campus and systemwide levels and can be split into those dealing with the setting of strategic direction for privacy and information security and those related to risk, compliance, and effectiveness of the privacy and information security programs. Meaningful execution of these responsibilities requires senior-level decision-making authority and appropriate administrative and academic representation for a unified approach to autonomy privacy, information privacy, and information security.

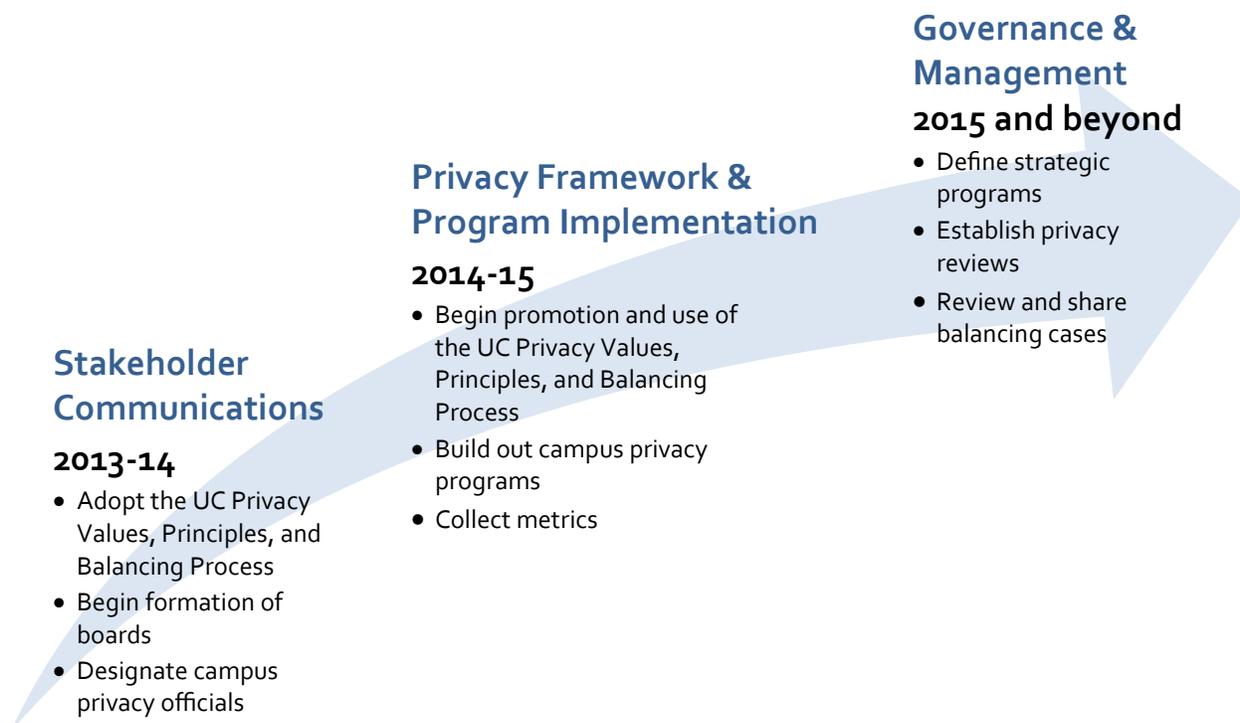
**RECOMMENDATION 4: Campus Privacy Official.** Each Chancellor should be charged with designating a privacy official to be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus. The privacy official shall work closely with the campus’s privacy and information security board.

A successful campus privacy program requires knowledgeable privacy leadership and an engaged campus community: the scope of privacy encompassed by the overarching privacy framework defined in this report is much larger than what is generally in place on campuses today. Designated privacy officials should be at a level able to effect organizational change within the University context of shared governance, mission, and values; and complex information technology infrastructure and operations. The privacy official will work with and be guided by the campus’s privacy and information security board on the vision, strategies, and methodologies of the campus privacy program; and collaborate with the UC Chief Information Security and Privacy Officer for systemwide alignment.

Infusing understanding and use of the UC privacy values and principles across the community in routine academic and administrative operations is fundamental to meeting the challenge of shifting expectations, new laws, and emerging technologies. A key responsibility of the campus privacy official will be to address this need.

### Proposed Implementation Schedule

Full adoption and implementation of the UC Statement of Privacy Values, UC Privacy Principles, Privacy Balancing Process, campus and systemwide boards, and designation of campus privacy officials will require four to five years to achieve a steady state. Recommendations for prioritizing the order and timing of key activities are summarized below.



---

# I INTRODUCTION

---

## Background

Privacy is fundamental to the University. It plays an important role in upholding human dignity and in sustaining a strong and vibrant society. Respecting privacy is an essential part of what it means to be a good citizen, whether as an individual or as an institution.

Academic and intellectual freedoms 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 where their ability to speak and to participate in discourse within the academy is possible without intimidation. Privacy is a condition that makes living out these values possible.

Privacy is also a basis for an ethical and respectful workplace, one that is as aligned with the culture and expectations of the millennial generation and beyond, as it is with today's workforce. Such a workplace becomes a competitive advantage for the University.

Privacy, together with information security, underpins the University's ability to be a good steward of the information entrusted to it by its 235,000 students and 185,000 employees, and by its extended community of patients, alumni, donors, volunteers, and many others.

Protecting privacy, however, is challenging—for many reasons. It is a complex and subtle concept that makes definition elusive. The "consumerization" of technology drives expectations of "anytime, anywhere" access to bank accounts, medical test results, personal data files, course materials, and professors; and speaks to work/life balance. The ubiquity of cellphone cameras exemplifies and underscores a shift in the ability of individuals to affect one another's privacy. Social media paradigms create vast virtual communities that intersect with "real" life in unexpected ways, many of them privacy related. Information such as browsing histories, IP addresses, and location information are routinely captured and may be correlated, contributing to a more comprehensive and invasive view of an individual's activity. The management and curation of "big data" introduces a new class of "information" requiring privacy considerations. Investigators—and their funding agencies and publishers—may consider data collected in the course of their research to be confidential, at least for a limited period of time, whether or not they are about individuals.

Information security, which protects both information and infrastructure, has become a formidable task, as a wide variety of devices—including those that are personally owned—access University systems and services. Privacy and information security legislation is proliferating and is anticipated to continue to add to the University's obligations, as are regulations about the collection, management, curation, and release of research data. The transparency required of public institutions can be in tension with the privacy of records about individuals and about research. How privacy is balanced against the many rights, values, and desires of our society is among the most challenging issues of our time.

In light of this situation and its rapidly changing context, in June of 2010, UC President Mark Yudof convened the University of California Privacy and Information Security Steering Committee to perform a comprehensive review of the University's current privacy and information security policy framework and to make recommendations about how the University should address near-term policy issues and longer-term governance issues. This goal was an overarching privacy framework that appropriately balances University values of individual privacy and academic freedom with other institutional obligations, including data protection.

The University of California has a rich foundation of principles and standards related to diversity, community, and ethics that guide the actions of a variety of constituents, including faculty, staff, students, partners, and collaborators. In addressing its charge, the Steering Committee leveraged

elements of the University’s culture, including its principles of community and investment in developing students who are informed and engaged citizens. Employing this foundation and providing leadership in privacy and information security, therefore, addresses President Yudof’s charge of protecting the values of both the University and its constituents.

## Approach and Deliverables of the Steering Committee

In examining the issues of privacy and information security in the context of the University of California, the Steering Committee reviewed relevant core concepts and principles and consulted with constituents and experts. A Working Group was formed to support the Steering Committee’s efforts by framing key issues and options for Committee discussion and turning those deliberations into concrete form.

The Steering Committee was guided by the following principles in considering its charge:

- We must maximally enable the mission of the University by supporting the values of academic and intellectual freedom.
- We must be good stewards of the information entrusted to the University.
- We must ensure that the University has access to information resources for legitimate business purposes.
- We must have a University community with clear expectations of privacy—both privileges and obligations of individuals and of the institution.
- We must make decisions within an institutional context.
- We must acknowledge the distributed nature of information stewardship at UC, where responsibility for privacy and information security resides at every level.

The Steering Committee’s deliverables comprise a set of recommendations responding to the four specific components of its charge<sup>1</sup>:

1. An overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;	All recommendations and definitions (page 9)
2. Governance, implementation, and accountability structures across the University with respect to privacy and information security;	Recommendations 2, 3, and 4
3. 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; and	All recommendations
4. Specific actions or phases needed to implement the proposed framework as University policy.	Section III, Proposed Implementation Schedule

The recommendations distill an expansive and nuanced examination of privacy frameworks employed in this country and internationally, of privacy models in use at other institutions as well as those articulated by leading privacy scholars, of the UC environment with respect to privacy, and of the

<sup>1</sup> The full charge can be found in Appendix A on page 27.

meaning of privacy itself (see Sources on page 42 for selected references). Where appropriate and beneficial, detailed analysis has been preserved to inform implementation of the recommendations made in this report. To date, no effort comparable in scope has been identified in higher education.

A primary goal of this report is to propose an integrated approach to privacy and information security. However, information security programs have greater maturity within the University. For example, whereas existing UC policy already requires the designation of an information security officer and implementation of an information security program, there is no equivalent for privacy. The apparent greater focus on privacy in this report is reflective of the relative states of privacy and security at UC at present.

The Committee entered this initiative with an expected focus on UC's current privacy policies. It emerged with a more holistic, integrated view of privacy—one that recognizes that privacy is as much directly about individuals (“autonomy privacy”) as it is about information *about* individuals (“information privacy”); that goes beyond compliance or any single policy, community, or role; and that acknowledges privacy and information security must be considered together. The recommendations presented here, therefore, drive toward a unified privacy model, led by the University's mission and values, against which existing guidance for decision-making, policy, and practice in the area of privacy and information security at the University of California can and should be aligned over time.

## Defining Privacy and Information Security

In developing its recommendations, the Committee identified a critical need to develop a common vocabulary to avoid confusion arising from differing interpretations of everyday words such as “privacy” or “governance”. Most crucial was the need to distinguish the intertwined concepts of *autonomy privacy*, *information privacy*, and *information security* from one another, and where necessary, make a decision about what definition to use. The Glossary on page 43 provides definitions of various terms as used in this report, but a more comprehensive definition of the three key terms follows.

**Privacy** is about the individual. In the context of this report, it is also about the agreement (“terms and conditions”) between the University and the individual that defines how privacy of that individual is handled.

Privacy comprises:

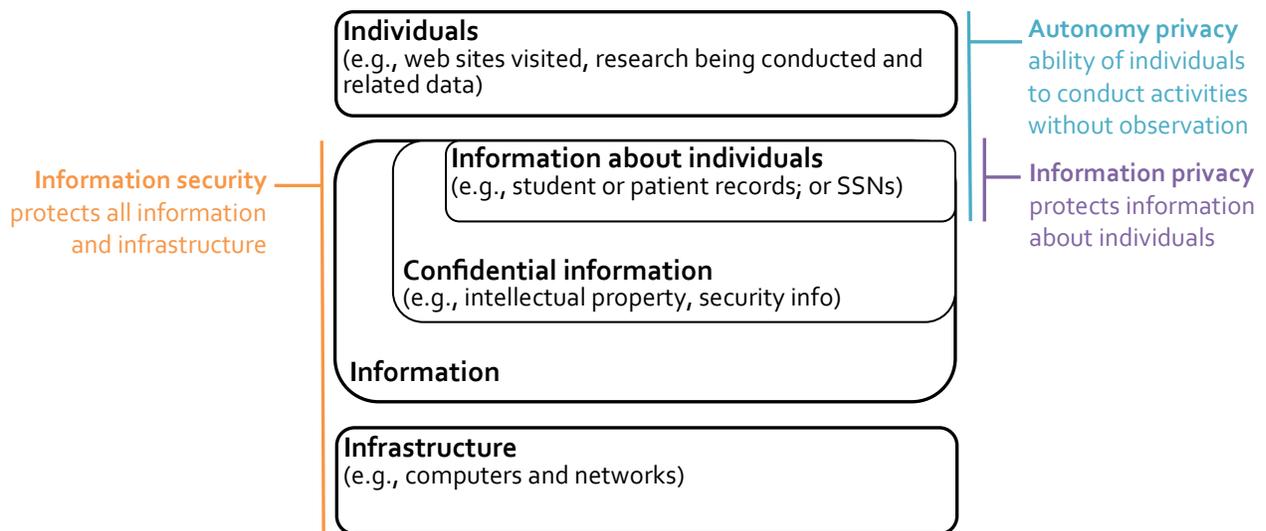
1. **Autonomy privacy:** an individual's ability to conduct activities without concern of or actual observation; and
2. **Information privacy:** the appropriate protection, use, and dissemination of information about individuals.

*Autonomy privacy* is an underpinning of academic freedom and is related to concepts such as the First Amendment's freedom of association, anonymity, and the monitoring of behavior; for example, by identifying with whom an individual corresponds or by building a profile of an individual through data mining. *Autonomy privacy* also encompasses records created by the individual such as research data, working drafts of research findings, communications of ideas, and opinions. It goes beyond the scope of (electronic) information and into the physical world when we speak of direct observation of individuals.

*Information privacy* is about an individual's interest in controlling or significantly influencing the handling of information about him or herself,<sup>2</sup> whether it is an academic, medical, financial, or other record.

**Information security** supports the protection of information resources from unauthorized access, which could compromise their confidentiality, integrity, and availability. Information resources include both infrastructure (such as computers and networks) and information (whether or not it is related to individuals). Information security supports, and is essential to, autonomy and information privacy.

These concepts are not as clear and independent as their definitions may suggest. The diagram below generally depicts the domains covered by autonomy privacy, information privacy, and information security, and the overlaps among them.



<sup>2</sup> Definition based from Clark, R. (see Source 1 on page 42).

## Observations

The University's long experience with privacy, when viewed through the lens of the new definitions presented in this report, reveals gaps, silos, and challenges in its approach to addressing privacy. This background has informed both the recommendations in this report and recognizes some of the related operational efforts under way.

A survey of privacy models identified those that spoke only to information privacy or, even more narrowly, to compliance with statutory or regulatory requirements—the traditional realm of the privacy officer—and not to autonomy privacy. Both forms of privacy are addressed in individual UC policies but have not been integrated into a policy framework; this report is intended to provide that framework. A key component for addressing operational integration is the UC Chief Information Security and Privacy Officer position hired in March 2012 (see Appendix B on page 30).

Another challenge is to promote convergence of the expectations of individuals with those of the University, which operates amid myriad legal and regulatory requirements, management demands, and operational issues. An individual, for example, may be willing to accept loss of personal information on a smartphone, whereas that phone may also contain information that the University is obligated to protect. These expectations are not easily reconciled under the University's existing policies. Individuals' expectations are based on different assumptions and constraints than are University policies. Technology, social norms, and policy evolve at differential rates.

The many UC policies related to privacy and information security were crafted at different times, and roles and responsibilities fall under different policy and organizational jurisdictions. Policy and organizational intersections create tensions rather than the integration necessary to address the full spectrum of present-day and future privacy concerns. This situation is compounded by the growth in privacy obligations, prevailing standards for due diligence that now expect proactive practices to prevent privacy breaches rather than reactive efforts if and when they occur, and in the number and variety of University partners to which the institutional commitment to privacy should extend. Consequently, a project to review the University's information security policies for consistency and alignment is being defined and will track the framework proposed in this report.

Although the campuses, medical centers, and national labs of UC are unified in their missions of teaching, research, and public service, they operate in a culture of relative autonomy. UC's operating model distributes stewardship and accountability across the organization, as evidenced by the number of privacy-related policies (see Appendix C on page 31) and the many campus offices that have stewardship of specific data (e.g., registrars, controllers, human resources, libraries, archives, and medical centers). The distributed nature of UC challenges the ability to look holistically at privacy and information security, and the recommendations in this report acknowledge this context in an effort to move the institution forward.

---

## II RECOMMENDATIONS

---

## UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process

**RECOMMENDATION 1: UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process.** The University shall formally adopt the proposed UC Statement of Privacy Values, Privacy Principles, and Privacy Balancing Process.

As its initial and overarching recommendation, the Steering Committee proposes the adoption of a UC Statement of Privacy Values, UC Privacy Principles, and Privacy Balancing Process, foundational elements integral to any privacy program. These elements may be expressed or implied in existing policy but have not been articulated in a consistent form that applies uniformly Universitywide.

1. The **UC Statement of Privacy Values** declares privacy—of both autonomy and information—as an important value of the University, as this is not explicitly done elsewhere; and clarifies that privacy is one of many values and obligations of the University. Such a statement is a peer to the UC Statement of Ethical Values,<sup>3</sup> Principles of Community,<sup>4</sup> and Diversity Statement.<sup>5</sup>
2. The **UC Privacy Principles** define a set of principles for the University that are derived from, and give concrete guidance about, the Statement of Privacy Values. These principles are a peer to the UC Standards of Ethical Conduct.<sup>6</sup>
3. The **Privacy Balancing Process** provides a mechanism for adjudicating between competing values, obligations and interests, whether as a tool in policy-making or to guide decision-making in specific situations, and even in a changing context.

By explicitly articulating these foundational elements outside the boundaries of any specific policy, functional area, or regulation, the intent is to create a unifying set of privacy expectations across the entire University community and provide a basis for achieving a common approach to privacy-related decisions – yet allow the flexibility that recognizes the University as a vast, complex organization with significantly varying needs and obligations that will change over time.

---

<sup>3</sup> [http://www.ucop.edu/ucophome/coordrev/policy/Stmt\\_Stds\\_Ethics.pdf](http://www.ucop.edu/ucophome/coordrev/policy/Stmt_Stds_Ethics.pdf)

<sup>4</sup> [http://www.universityofcalifornia.edu/diversity/principles\\_community.html](http://www.universityofcalifornia.edu/diversity/principles_community.html)

<sup>5</sup> <http://www.universityofcalifornia.edu/diversity/diversity.html>

<sup>6</sup> <http://www.universityofcalifornia.edu/compaudit/ethicalconduct.html>

## 1. UC Statement of Privacy Values

### Overview

The UC Statement of Privacy Values first declares privacy as an important value of the University of California. It then defines what the two forms of privacy are, and explains that they must be balanced with one another and with other values and obligations of the University. To give context, the values of academic and intellectual freedom are highlighted as fundamental to an educational and research institution; and the values of transparency and accountability are highlighted as fundamental to a public institution. Finally, a summary of elements that the University strives to balance appropriately is given.

### The UC Statement of Privacy Values

The University of California respects the privacy of individuals. Privacy plays an important role in human dignity and is necessary for an ethical and respectful workplace. The right to privacy is declared in the California Constitution.

Privacy consists of (1) an individual's ability to conduct activities without concern of or actual observation and (2) the appropriate protection, use, and release of information about individuals.

The University must balance its respect for both types of privacy with its other values and with legal, policy, and administrative obligations.

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

Transparency and accountability are values that form the cornerstone of public trust. Access to information concerning the conduct of business in a public university and an individual's access to information concerning him/herself is a right of every citizen as stated in the California Constitution.

Thus, the University continually 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;
- being an attractive place to work;
- honoring its obligation as a public institution to remain transparent, accountable, and operationally effective and efficient; and
- safeguarding information about individuals and assets for which it is a steward.

## 2. UC Privacy Principles

The proposed UC Privacy Principles are derived from the UC Statement of Privacy Values and from established privacy principles, such as the Organisation for Economic Co-operation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data<sup>7</sup> and the Federal Trade Commission’s (FTC) Fair Information Privacy Practice Principles.<sup>8</sup> The UC Privacy Principles are intended to guide policies and practice in conjunction with well-understood information security objectives of protecting the confidentiality, integrity, and availability of information resources.

The UC Privacy Principles consist of principles that address both autonomy privacy and information privacy, as follows:

### Autonomy Privacy Principles

Members of the University community are expected to uphold autonomy privacy, which is the ability of an individual to exercise a substantial degree of control over one’s expressions, associations, and general conduct without unreasonable oversight, interference, or negative consequences. In the University setting, autonomy privacy is closely associated with the concepts of academic freedom, free speech, and community. The following proposed autonomy principles are intended to capture our culture of openness, transparency, ethical behavior, and respect for others:

Free inquiry	The University is guided by First Amendment principles and is committed to encouraging its members to exercise free discourse without fear of reprisal or intimidation, subject to the privacy and safety of other individuals or University resources.
Respect for individual privacy	The University is committed to respecting the privacy of individuals, including their interactions with others, and expects University members to esteem each other’s privacy and well-being.
Surveillance	The University is guided by Fourth Amendment principles regarding surveillance of persons or places, whether in person on campus or electronically, and is committed to balancing the need for the safety of individuals and property with the individuals’ reasonable expectation of privacy in a particular location.

<sup>7</sup> [http://www.oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)

<sup>8</sup> <http://www.ftc.gov/reports/privacy3/fairinfo.shtm>

## Information Privacy Principles

The University is committed to providing individuals with a reasonable degree of control over the collection, use, and disclosure of information about themselves. The following principles provide guidance to the University for incorporating information privacy into its policies and practices:

Privacy by design	<p>The University is committed to building privacy protections that embody the additional principles stated below into its business processes and information systems associated with the collection, use, and disclosure of information about individuals and about confidential information for which individuals are responsible. Business processes and information systems initiatives, revisions, or upgrades will be evaluated for consistency with the UC Privacy Principles and compliance with associated policies.</p>
Transparency and notice	<p>The University demonstrates its commitment to transparency by giving individuals reasonable advance notice of its information policies and practices for collecting, using, disclosing, retaining, and disposing of information about individuals.</p> <p>The University expects its members to collect, use, disclose, and retain only the minimum amount of information about individuals as necessary for the specified purpose and to appropriately dispose of such information in accordance with the University's records-retention schedules.</p> <p>The University expects its members who collect information about individuals to publish privacy notices that clearly inform individuals about the purposes (how information will be used or disclosed as permitted or required by law) and the scope of information collected.</p>
Choice	<p>Prior to collecting, using, disclosing, or retaining information about individuals, the University expects its members to provide individuals, whenever possible, with the ability to choose whether to and by what means to provide their information.</p> <p>However, when the information about the individual is necessary to deliver a service or benefit or to participate in an activity, the individual may be required to provide the information in order to receive the service or benefit or to participate.</p>
Information review and correction	<p>Unless prohibited by law, the University is committed to providing individuals with a way to review the information about themselves that they have provided or permitted to be collected, as well as a procedure to request the correction of inaccuracies and one to perform the correction if appropriate.</p>

Information protection	The University demonstrates its commitment to protecting information about individuals under its stewardship by providing appropriate employee training and by implementing privacy and information security controls.
Accountability	<p>The University expects every individual to be aware of and accountable for complying with these principles and actively supporting the University's commitment to respect the privacy of individuals.</p> <p>The University demonstrates its commitment to these principles by investigating reported violations of information privacy principles and policies and, as appropriate, taking corrective measures.</p>

### 3. Privacy Balancing Process

The Privacy Balancing Process is intended as a tool to guide policy-making and decision-making when competing privacy interests, University values, or obligations exist and for which no statutory provision, common law, or University policy is directly applicable. The balancing process is derived from the UC Privacy Statement, applies the UC Privacy Principles, and rests on the acknowledgement that protecting autonomy privacy depends both on protecting information privacy and on ensuring information security.

The balancing process is intended to achieve consistency in privacy-related decisions. The process will be employed by governance bodies (described subsequently) in such a way that a cumulative body of institutional knowledge will inform policy development and routine practices of campus privacy officials and other UC managers. The process is applicable both to information that the University maintains about individuals (information privacy); as well as to their speech and behavior that is conducted on University premises, that uses University resources, or that is made in their role as a University representative (autonomy privacy).

A balancing decision depends on the specifics of each case, weighing multiple interests and impacts. The relative weights of many factors are analyzed to determine whether the proposed course of action is sufficiently compelling to justify the impacts. For example, proposals to monitor or to collect information about the activities of individuals must articulate a significant University or individual need for such activity. Such a “significant interest” stance gives reasonable deference to the privacy of individuals without unduly constraining institutional operational needs.

The balancing process analysis may result in a conclusion that one party’s interest or position carries the most weight. For example, a University’s policy to require individuals to identify themselves before entering certain campus buildings is approved because the University’s obligation to protect the physical safety of individuals on campus outweighs an individual’s privacy interest in anonymity. The balancing process could also result in striking a balance between the different interests, finding an acceptable middle ground that gives deference to each interest. The balancing process allows the University to remain flexible in light of changes in laws, societal norms, technological change, individual expectations, and University needs.

#### Privacy Balancing Analysis Factors

The balancing process must expressly consider the parties’ interests, benefits, burdens, and consequences associated with the proposed action. Each analysis will differ depending on the action and the interests involved. A “party” in such an analysis may be, or represent, an individual, a community, or the University; with the recognition that parties may overlap or that a party may have multiple roles.

Some potential factors that are helpful to privacy analysis are given below. This list is not intended to be prescriptive; it is intended to illustrate how a balancing analysis would be conducted.

- What are the benefits to each party in successfully asserting privacy interests or a specific policy stance? What are the burdens, impacts, and risk to each party if the proposed action is not taken?
- What alternative approaches, or reasonable privacy protections, might be used in conjunction with the proposed action to make it less intrusive?
- What are the costs, whether in dollars, time, effectiveness, or other metrics?

- What actions have been taken (or could be taken) by each party to protect their own interests?
- What new technologies or processes might mitigate the privacy concerns, now or in the foreseeable future?

### Building Consistency into the Process

The balancing process is inherently subjective. The analysis is based on the facts of each situation, the factors selected to weigh the parties' interests, and the outcome of similar cases. It is more flexible than rules-based decision-making and expressly allows the full circumstances of the parties to be considered. The cost of such flexibility, however, is that similar cases may not be treated in the same way or result in the same outcome. To address this aspect of the balancing process, the University should adopt a case review process whereby the analysis and rationale supporting the University's balancing decisions are reviewed periodically. In addition, a mechanism should be developed for particularly well-reasoned decisions to be shared among campuses and recommended as guidelines for similar situations, without disclosing information of the individuals involved in the matter.

## Campus Privacy and Information Security Boards

**RECOMMENDATION 2: Campus Privacy and Information Security Boards.** Each Chancellor shall form a joint Academic Senate–Administration board to advise him or her, or a designee, on privacy and information security; set strategic direction for autonomy privacy, information privacy, and information security; champion the UC Privacy Values, Principles, and Balancing Process; and monitor compliance and assess risk and effectiveness of campus privacy and information security programs.

High-level campus privacy and information security boards with Academic Senate, administrative, and student representation should be formed on every campus to bring domain expertise and critical viewpoints to local governance,<sup>9</sup> sending a clear message that UC is serious about protecting the privacy of its students, academic and staff employees, patients, and the public.

### Campus Board Responsibilities

#### Setting strategic direction

- Setting strategic direction in the areas of privacy and information security for the campus; considering issues in these areas and their impact on the campus and the communities it serves
- Staying current on new developments in privacy and information security, including related technology developments
- Recommending issues for systemwide consideration as appropriate

#### Risk, compliance, and effectiveness

- Application of the privacy balancing process to resolve competing interests
- Assembling, reviewing, and approving the sharing of balancing analyses among campuses<sup>10</sup>
- Ensuring that the campus privacy program delivers fair and consistent decisions
- Ensuring that the campus privacy and information security programs have sufficient visibility and executive support
- Monitoring campus compliance with UC Privacy Values and Principles
- Assessing the effectiveness of the campus privacy and information security programs
- Reporting annually for transparency

### Campus Board Structure

Campus boards should reflect a wide range of expertise.

- Academic representatives should be appointed for terms of sufficient length to provide for continuity and to build cohesiveness and institutional memory. A formal link to the Academic Senate is required and a robust feedback loop with the Senate is part of the role.
- Administrative representatives must include the designated privacy official and information security officer and a link with the Campus Ethics, Compliance, and Risk Committee.

<sup>9</sup> The UCLA Board on Privacy and Data Protection (see page 35 in Appendix D) is an example of how such a body may be structured and function. Several other campuses have or are in the process of forming similar committees, though often structured as subcommittees of the local Campus Ethics, Compliance and Risk Committee.

<sup>10</sup> See “Building Consistency into the Process” on page 19.

## Systemwide Board for Privacy and Information Security

**RECOMMENDATION 3: Systemwide Board for Privacy and Information Security.** The President shall form a joint Academic Senate–Administration board systemwide to advise him or her, or a designee, on privacy and information security; set strategic direction for autonomy privacy, information privacy, and information security; steward the UC Privacy Values, Principles, and Balancing Process; and monitor their effective implementation by campus privacy and information security boards.

A privacy and information security approach with transparent strategic objectives will help to foster a culture that respects privacy at the University and aligns with the University’s mission, vision, and values. A systemwide board would provide a consistent approach to managing issues and conflicts, cohesive policies and practices, and a decision-making framework that is logical, repeatable, and structured. It would also lead to decisions that define and clarify expectations that align with the University’s mission and its privacy values and principles.

### Systemwide Board Responsibilities

#### Setting strategic direction

- Setting strategic direction in the areas of privacy and information security, considering issues in these areas and their impact on the University and the communities it serves
- Approving changes to the UC Privacy Values, Principles, and Balancing Process as necessary to keep them aligned with legislation, best practices, new technology, emerging risks, and other critical privacy drivers within the context of the strategic directions

#### Risk, compliance, and effectiveness

- Ensuring the timely and responsive implementation of the UC Privacy Values, Principles, and Balancing Process across the University
- Monitoring the ongoing effectiveness of implementation by campus privacy and information security boards
- Reporting annually for transparency

### Systemwide Board Structure

The Systemwide board should reflect a broad range of expertise and include broad campus representation.

- Academic: Senior Academic Senate leadership.
- Administrative: Provost and Senior Vice President, Academic Affairs; Senior Vice President and Chief Compliance and Audit Officer; Chief Information Officer and Associate Vice President, Information Technology Services; Systemwide Chief Information Security and Privacy Officer.
- Representation from the campuses.

## Campus Privacy Official

**RECOMMENDATION 4: Campus Privacy Official.** Each Chancellor shall designate a privacy official to be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus. The privacy official shall work closely with the campus's privacy and information security board.

The scope of privacy encompassed by the overarching privacy framework defined in this report is much larger than what is generally in place on campuses today. A successful campus privacy program requires knowledgeable privacy leadership and an engaged campus community. Each Chancellor should designate a privacy official with responsibility for the development and administration of a unified campus privacy program. The privacy official should be at a level able to effect organizational change within the University context of shared governance, mission, and values; and complex information technology infrastructure and operations.

The privacy official shall work closely with the campus's privacy and information security board on the vision, strategies, and methodologies of the campus privacy program; and collaborate with the campus's information security officer<sup>11</sup> and other functional experts, and the UC Chief Information Security and Privacy Officer for systemwide alignment.

A campus privacy program encompasses viewpoints and expectations from the campus community and the legal and technological landscapes and addresses both autonomy and information privacy in:

- Identifying and managing privacy risks;
- Developing privacy policies and practices;
- Maintaining integrity over campus practices and decisions that impact privacy;
- Fostering privacy by design;
- Properly handling privacy breaches;
- Resolving conflicting privacy interests and ensuring the application of the balancing principles where appropriate; and
- Actively exploring technologies and methods that can help to protect privacy.

Infusing understanding and use of the UC privacy values and principles across the community in routine academic and administrative operations is fundamental to meeting the challenge of shifting expectations, new laws, and emerging technologies. A key responsibility of the campus privacy official will be addressing this need, whether in clarifying the boundaries of personal privacy, which is at the heart of the complex and vexing issue of the commingling of University information with personal information, or in promulgating the expectation that University privacy and information security principles extend to relationships with partners and collaborators.

---

<sup>11</sup> Business and Finance Bulletin IS-3 defines a policy basis for a UC information security program that includes identification of an individual to perform the function of Information Security Officer (ISO) "designated on each campus to be responsible for its Program. Responsibility for compliance with this bulletin will rest with a number of individuals, and the ISO must facilitate this compliance through collaborative relationships with academic and administrative officials, consistent with campus governance structure and policy compliance strategies." Organizational strategies to implement the ISO function will vary by campus. This is also true for privacy officials. For example, a medical center will likely have its own privacy official, with coordination between like roles.

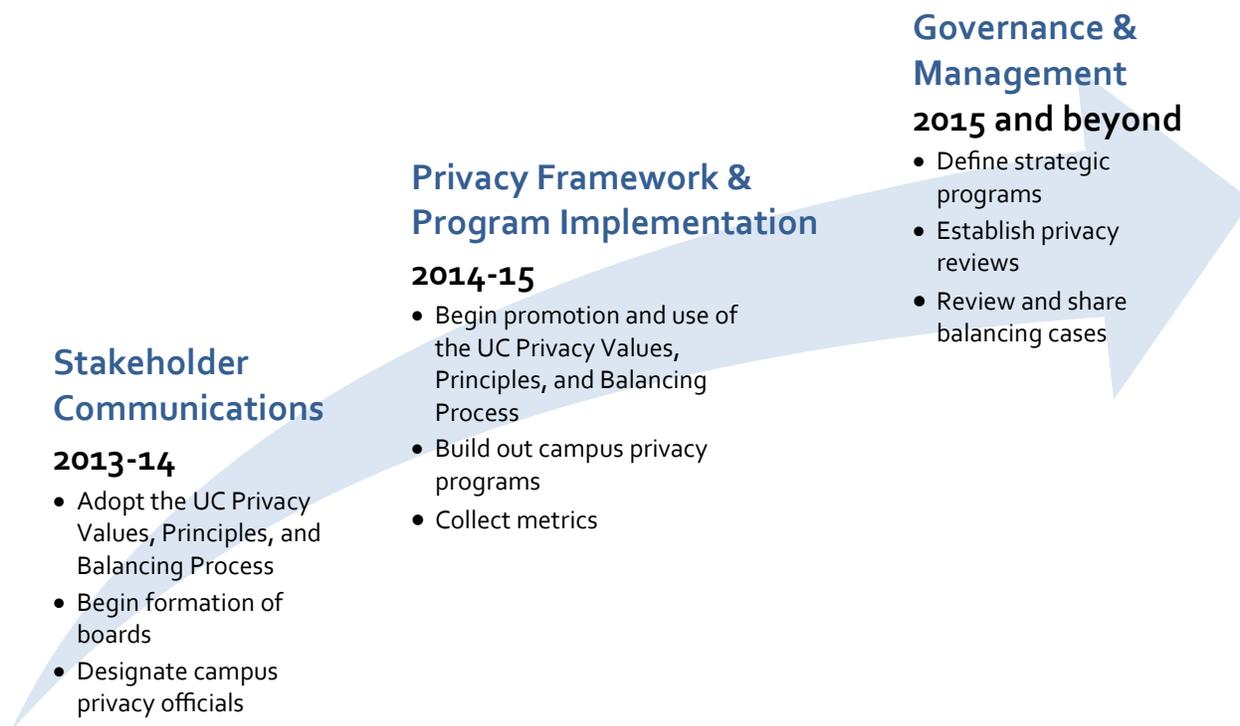
---

## **III PROPOSED IMPLEMENTATION SCHEDULE**

---

## Overview

Full adoption and implementation of the UC Statement of Privacy Values, UC Privacy Principles, Privacy Balancing Process, campus and systemwide boards, and designation of campus privacy officials will require four to five years to achieve a steady state. Recommendations for prioritizing the order and timing of key activities are summarized below.



### Year 1: Stakeholder Communications

The first year of implementation focuses on stakeholder communications to announce and promote the University's commitment to privacy; describe the UC Statement of Privacy Values, Privacy Principles, and Balancing Process; form the campus and systemwide boards; and designate campus privacy officials. Because the overarching privacy framework defined by the four recommendations proposed in this report is unique in the industry, it is expected to generate a high level of interest from other universities and from the privacy press.

During the first year, campuses will benefit from support to help them define and organize their privacy programs and maintain the anticipated level of consistency and quality. Coordination from the UC system should occur, along with privacy official training and education and consistent systemwide messaging.

### Years 2-3: Privacy Program Implementation

The next two years cover the majority of initial implementation activities. The communications program should shift from announcement and explanation to expectations and how internal processes are changing. Policy alignment should be significantly underway. Privacy officials and campus and

systemwide boards should have completed their training and have some experience using the balancing process. Governance boards should be planning for initial program reviews and defining the metrics that guide and determine success. At the end of this initial implementation, policy and process will be visible at the campus; privacy officials will be in place; and boards will be setting directions and working with campus operations to integrate privacy into operational practices.

### Years 4-5: Sustainable Privacy and Information Security Governance and Management

By year four, the privacy officials will be working closely with campus operations to implement privacy policy and best practices. Operational units with significant privacy risks will have established their own privacy liaison roles. These individuals will be working closely with the privacy officials and program staff. The boards will be actively engaged. Campus discourse about privacy and how to engage in balancing analysis will be active and influential in major campus decisions. Privacy practices will be shared across campuses, and UC best-practice recommendations will be emerging. By year five, privacy will be ingrained as part of the UC way of life.

---

# APPENDICES

---

## Appendix A. Steering Committee Charge

1111 Franklin Street  
Oakland, California 94607-5200  
Phone:(510)987-9074  
Fax: (510) 987-9086  
<http://www.ucop.edu>

June 30, 2010

Dear

I am convening the University of California Privacy and Information Security Steering Committee to perform a comprehensive review of the University's current privacy and information security policy framework and to make recommendations about how the University should address related near-term policy issues and longer-term governance issues.

I am writing to invite you to become a member of the Steering Committee, which will be chaired by UC Santa Barbara Executive Vice Chancellor Gene Lucas, with support from Senior Vice President Sheryl Vacca and Associate Vice President David Ernst. Senior Vice President Vacca and Associate Vice President Ernst will appoint a working group to support the Steering Committee with issue analysis and document preparation. Their office staffs will handle logistics for both groups. I enclose a copy of the proposed membership list for your information.

A pressing reason for this review is the University's immediate need to ensure the privacy of confidential information in our care. The University is obligated by law and as a steward of the public trust to protect confidential information, such as patient medical records, employee personal information, and research participant data. At times, technical methods for protecting data, such as scanning or filtering e-mail, conflict with University principles expressed in the Electronic Communications Policy (ECP), such as the affirmation that the University does not monitor electronic communications without the holder's consent. Given this conflict and our obligations, the University must develop and issue clear guidance about data protection and legal compliance in the context of individual privacy and freedom of expression. I enclose a background statement that provides additional discussion of these issues.

The Steering Committee will shape the scope and direction of its work, including revising membership, refining key objectives, and establishing short- and long-term timelines. The Steering Committee will also review core concepts and principles, consult broadly with constituents and experts, and, within eighteen months, provide me with a set of recommendations. Specifically, the charge to the Committee is 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.

Privacy principles touch the heart of the academic enterprise, and the University must address business needs within that context. Therefore, I have sought individuals for the Steering Committee who will represent both academic and business perspectives. Members will be responsible for broadly

communicating with and receiving input from their peer groups and constituents about the Steering Committee's goals, process, and recommendations.

I appreciate your willingness to participate in this important endeavor. Executive Vice Chancellor Lucas will be in touch with you over the summer to schedule the first meeting of the Committee this fall.

With best wishes, I am,

Sincerely yours,

Mark G. Yudof  
President

Enclosures

cc: Chancellors

Senior Vice President and Chief Compliance and Audit Officer Vacca

Associate Vice President and Chief Information Officer Ernst

Executive Vice Chancellor Lucas

## Problem Statement

The University of California urgently needs to create an overarching privacy and information security policy framework that appropriately balances University values of individual privacy and academic freedom with other institutional obligations, including data protection.

The University of California Electronic Communications Policy (ECP) is the primary University policy governing principles of individual privacy, or civil liberties. Importantly, the ECP establishes that the University of California does not monitor the content of electronic communications, thereby affirming the institution's commitment to academic freedom, freedom of expression, and freedom from censorship. Other University policies also address such privacy issues as data protection, records management, information security, compliance with the California Public Records Act, etc. As a result, University guidance on privacy is not integrated into a unifying framework that is clear and accessible to every member of the University community, thus enabling compliance with both University principles and state and federal law. The result of this fragmented approach is insufficient guidance when policies conflict, divergent practices across the system, and a complicated policy environment that does not readily adapt to address emerging issues and evolving institutional needs.

The world has changed in many ways since the ECP was issued nearly ten years ago. A primary change has been that massive amounts of confidential data—including personal health information, Social Security numbers, and financial account information—are now created, transmitted, and stored in electronic form. At the same time, the number and scope of data breaches have grown and are a major concern. Key ECP concepts, such as the provision for incidental personal use of University electronic communications resources, at times conflict with such institutional obligations as the protection of confidential data, or business management and accountability.

This changing context calls for a thoughtful consideration of emerging issues. A critical issue at present is the University's need to protect confidential data from inappropriate access or use. In many instances this is a legal obligation; in others it simply reflects the University's responsibility as a good steward of sensitive data. Proposed data protection measures, however, may involve the monitoring of electronic

communications and transactions and hence conflict with the privacy provisions of the ECP. This puts University organizations in a difficult position. They urgently need clear guidance now so they may meet legal and stewardship obligations without violating University privacy principles.

Perhaps more importantly, the University needs a policy framework that over time provides for review of key issues as well as policy revision where necessary to address the evolution and intersection of technology, law, and culture in the University environment. To this end, President Yudof has established a systemwide University of California Privacy and Information Security Steering Committee to provide a formal structure and process for discussion of evolving privacy and information security issues and development of systemwide policies and guidance.

## Definitions of Privacy in the University Context

The term privacy is used in two distinct though related senses. One refers to civil liberties, the other to data protection and systems security. Both types of privacy are important to the University but there is inherent tension between them. Information security is necessary to protect privacy, but some information security measures intrude upon privacy.

- *Civil Liberties Sense:* This sense involves protecting the privacy of individuals and their right to be free from “big brother,” surveillance, and monitoring. This type of privacy underpins University values of academic freedom and freedom of speech. It reflects human behavior with respect to the ethical collection, use, sharing, protection, and retention of personal information.
- *Data Protection and Systems Security Sense:* This sense involves protecting confidential data about individuals from unauthorized disclosure as well as protecting systems and network infrastructure and services for reliability and integrity. Security encompasses systems, processes, and procedures governing the confidentiality, integrity, and availability of information assets.

## Purpose of UC Privacy and Information Security Initiative

Through the UC Privacy and Information Security Initiative, the University will review existing privacy and information security policies; develop a new overarching policy framework to address privacy and information security in the modern legal, technology, and social context; and provide clear updated guidance to assist the University community in meeting legal obligations to safeguard “protected” data while at the same time abiding by deeply held principles of privacy.

This review will be conducted on a broadly consultative, systemwide basis, drawing from expertise within the University academic community and outside the University system as well. The review is expected to result in recommendations for policy and, as necessary, changes in governance and accountability for privacy and information security policy implementation. To the degree possible, these recommendations will seek to resolve or minimize conflict between University privacy principles and data protection obligations and, ultimately, position the University to continue to fulfill its most important responsibility—adherence to principles of academic freedom.

## Appendix B. UC Chief Information Security and Privacy Officer

David J. Ernst  
CIO and Associate Vice President  
University of California Office of the President

November 8, 2011

Subject: Appointment of UC Chief Information Security and Privacy Officer

Dear Colleagues:

I am pleased to announce the appointment of Cheryl Walton Washington to the position of Chief Information Security and Privacy Officer at the University of California Office of the President. Cheryl has over twenty year experience working in higher education and currently is the Chief Information Security Officer for the California State University (CSU) system. She will assume her UC position in March 2012 in order to transition from several major projects she currently is leading for CSU. This fall and early winter, Cheryl will spend some time getting to know UC colleagues and learning about the university's information security and privacy position and establishing goals so that she will be ready to hit the ground running in March.

The Chief Information Security and Privacy Officer is a new position that, for the first time, will provide a systemwide coordinating function for information security and privacy in support of campus needs in these areas. Cheryl will be responsible for collaborating with campus counterparts to establish and maintain a universitywide information security and privacy program to safeguard and manage information security assets and personal or protected information. She also will serve as the Information Security Officer for UCOP, and will direct information security within the UCOP Information Technology Services department. She reports to me and also has a dotted line reporting relationship to Chief Compliance Officer Sheryl Vacca. On behalf of SVP Vacca, she will coordinate with the Systemwide Health Sciences Privacy Liaison on information security and privacy initiatives that impact health sciences and the medical centers.

Cheryl is very excited about returning to UC in this new and critical role. Early in her career, she held IT positions at UCB and UCOP. At CSU, she has had experience addressing information security from the perspective of a campus, as Information Security Officer for CSU East Bay campus and, currently, from the perspective of the system, as systemwide ISO. In her present role, Cheryl works closely with academic, business, information security, and IT leadership teams to develop and implement CSU's information security vision and strategy as well as to address privacy issues. She holds certifications as an information privacy professional, information security manager, and information system auditor. I am sure you will enjoy working with her. Please join me in welcoming Cheryl to UC.

Best,

David

## Appendix C. Existing Systemwide Policies Related to Privacy and Information Security

---

### General documents

---

Faculty Code of Conduct, Student Conduct Code  
Statement of Ethical Values, Diversity Statement, Principles of Community

---

### Academic Personnel Manual

---

APM-110	Academic Freedom	Autonomy privacy
APM-160	Maintenance of, Access to, and Opportunity to Request Amendment of Academic Personnel Records	Information privacy

---

### Presidential policy

---

ECP <sup>12</sup>	Electronic Communications Policy	Autonomy privacy: Academic freedom, subpoenas, search warrants
-------------------	----------------------------------	--

---

### Business and Finance Bulletins: Information Systems

---

IS-2	Inventory, Classification, and Release of University Electronic Information	Information privacy, information security: Release and disclosure requirements, risk assessment
IS-3 <sup>13</sup>	Electronic Information Security	Information security program elements, CA Information Practices Act/breach notification
IS-10	Systems Development Standards	Information security
IS-11	Identity and Access Management	Information security

---

<sup>12</sup> The ECP, since its formal adoption in 1998 (and through the UC Email Policy prior to that), has served as the University's de facto privacy policy, articulating governing principles for individual privacy. The ECP establishes that UC does not monitor the content of electronic communications except under limited circumstances, thereby affirming the institution's commitment to academic freedom, freedom of expression and freedom from censorship.

<sup>13</sup> IS-3, adopted in 1998, essentially defines an information security program for the University. It articulates guidelines for achieving appropriate protection of University electronic information resources and the identification of roles and responsibilities.

**Business and Finance Bulletins: Records Management and Privacy Series<sup>14</sup>**

RMP-7	Privacy of and Access to Information Responsibilities	Information privacy
RMP-8	Legal Requirements on Privacy of and Access to Information Policy on Disclosure of Compensation Information	Information privacy: FERPA, Privacy Act, California Information Practices Act California Information Practices Act
RMP-9	Guidelines for Access to University Personnel Records by Governmental Agencies	Information privacy
RMP-11	Student Applicant Records	Information privacy
RMP-12	Guidelines for Assuring Privacy of Personal Information in Mailing Lists and Telephone Directories	Information privacy

**Business and Finance Bulletins: Business Affairs**

BUS-43	Materiel Management	Information privacy, information security: Contract language for third-party data protection and breach notification requirements
BUS-49	Policy for Cash and Cash Equivalents Received: Appendix B, Data Security	Information security: Data security and access management, Payment Card Industry Data Security Standards
BUS-80	Insurance Programs for Information Technology Systems	UC Cyberinsurance program: coverage and requirements

**Other domain-specific policies**

HIPAA policies	Nine policies and glossary	HIPAA
FERPA policies	UC Policies Applying to the Disclosure of Information from Student Records Student Privacy Policy on Photographs and Recordings	FERPA

Policies implementing other specific laws and regulations, such as ADA, GLBA and Red Flags  
Policies on human subjects research, personnel, sexual harassment and whistleblower cases

<sup>14</sup> The Records Management Program, established in 1963 by UC President Clark Kerr, includes the Records Management and Privacy (RMP) policy series that articulate the policy, regulations and general principles for appropriately managing, accessing and preserving administrative records throughout their life cycle and provides schedules for their final disposition.

## Appendix D. Existing Campus Privacy and/or Information Security Committees

### UC Davis Information Privacy and Security Subcommittee Charter

#### A. Subcommittee Composition

The Information Privacy and Security Committee members are appointed by the Provost and Executive Vice Chancellor and shall include the following members:

<b>Co-chairs</b>	<ul style="list-style-type: none"> <li>• Campus Information Technology Security Coordinator</li> <li>• Campus Chief Compliance Officer</li> </ul>
<b>Members</b>	<ul style="list-style-type: none"> <li>• Campus Information Technology Security Coordinator</li> <li>• Chief Compliance Officer – General Campus</li> <li>• Manager of IT Audit, Internal Audit Services</li> <li>• An academic unit representative from Senior Advisors</li> <li>• A representative from the Academic Senate</li> <li>• A representative of the Deans Technology Council, on behalf of the DTC and Technology Infrastructure Forum</li> <li>• A representative from the Coordinating Council of the Domain Conveners</li> <li>• Campus Counsel</li> </ul>

The Campus Information Technology Security Coordinator and campus Chief Compliance Officer will co-chair the Subcommittee. The Subcommittee will meet every other month or more frequently, as required. A majority of voting members must be present to conduct a meeting. The subcommittee may conduct business outside of regularly scheduled meetings when the co-chairs of the subcommittee deem it necessary. Subcommittee members will act broadly in the interest of the campus and on behalf of the organization from which they are drawn. There is an expectation that subcommittee members will consult and share information with their organization and others, where appropriate.

The Subcommittee will form workgroups to address privacy issues as needed.

#### B. Purpose

The Information Privacy and Security Subcommittee meets regularly to evaluate campus policies regarding information privacy and cybersafety and risks associated with threats to cybersafety and related potential invasions or breaches of personal privacy information. The Information Privacy and Security Subcommittee will recommend strategies for minimizing risks and improving compliance with campus and systemwide information privacy and cybersafety policies and procedures.

#### C. Responsibilities

The Subcommittee:

1. Reviews information privacy and cybersafety policies and standards as well as cybersafety surveys, analysis of survey responses, and risk assessments prepared by Information and Educational Technology (IET) and the results of privacy and cybersafety related audits performed by Internal Audit Services (IAS) and/or external auditors.

2. Recommends revisions and improvements to campus information privacy and cybersafety policies and standards.
3. Develops, guides and monitors campus transition plans to the broad use of common security solutions with input from the campus community.
4. Based on information provided by IET, IAS and external auditors and in consultation with the campus community, evaluates cybersafety risks to the campus and develops recommended strategies for mitigating those risks.
5. Reviews campus compliance with systemwide privacy and security policies and, where needed, develops recommended strategies for compliance improvement.
6. Reviews all proposals submitted under the Development and Review of Administrative Computing Systems (PPM 200-45) for privacy and security related issues and mitigation plans.
7. Serves as a resource for privacy and security related initiatives managed through campus-wide security services.
8. In the event of a suspected or alleged breach of state or federal privacy laws, serves as a resource to assist campus administrators in investigating, evaluating and responding to the alleged or suspected breach.
9. Maintains awareness of current privacy and security issues within higher education.

#### D. Reporting

The Subcommittee reports to the Provost and Executive Vice Chancellor and the Campus Ethics and Compliance Risk Committee (CECRC). On an annual basis, the Subcommittee provides a written report to the CECRC addressing privacy and cybersafety risks to the campus, the severity of those risks and recommendations for mitigating those risks. Reports shall be made on a more frequent basis when deemed necessary by the Subcommittee or requested by the CECRC.

## UCLA Board on Privacy and Data Protection

### A. Purpose and Charge

The Board is charged with articulating institutional positions on privacy and data protection reflecting the campus's values and cultural expectations to guide policy development and decision-making. It is the campus nexus for considering initiatives, proposals and stances that must balance privacy, data protection and the campus's other values and obligations (e.g., openness, accessibility, emerging technology trends, legal obligations, and individual expectations).

### B. Authority

Executive Vice Chancellor and Provost

### C. Membership

Privacy is essential to academic freedom and to the conduct of teaching and research. The Board is therefore organized in structure and process to reflect the faculty voice and the Academic Senate must play a vital role in the governance of privacy and data protection for the academy.

The Board maintains a balanced number of faculty and administration, plus one graduate and one undergraduate student representative. Faculty appointments should ensure social, cultural, technical and management aspects of privacy and data protection. Administrative appointments should have direct involvement with institutional management of privacy matters.

Members are recommended by the Board's Executive Committee, in consultation with the full Board, and require a majority vote to be confirmed. The Executive Committee is responsible for managing the recommendation process.

#### Voting Membership

##### *Faculty*

- Faculty members equal to the number of administrative voting members (staggered three-year terms).
- The Chair-Elect of the Academic Senate shall be included and counted as one of these members. [Under discussion]

##### *Students*

- One undergraduate student designated by the Undergraduate Students Association Council (one year term)
- One graduate student designated by the Graduate Students Association (one year term)

##### *Administration*

1. University Librarian
2. Vice Provost, Information Technology
3. Designee from the Office of the Campus Counsel
4. Chief Compliance Officer of the Medical Center
5. University Registrar
6. Director, Office of the Human Research Protection Program
7. Designee from Campus Human Resources

### Non-Voting Membership

1. UCLA Chief Privacy Officer
2. UCLA Chief Information Security Officer
3. Designee of the Executive Vice Chancellor and Provost
4. Designee from Audit & Advisory Services

### D. Executive Structure

- *Faculty Chair (two-year term)*: The Chair must be a voting faculty Board member, ladder faculty and appointed by both the Executive Vice Chancellor and Provost and the Academic Senate.
- *Administration Vice Chair (two-year term)*: The Vice Chair must be a voting administrative Board member.
- *Executive Committee*: The Executive Committee comprises the Chair, Vice Chair and UCLA Chief Privacy Officer. It acts on behalf of the Board to ensure responsiveness with regard to operations and agendas.

### E. Representation to Oversight Committee

The Chair and/or the Vice Provost, Information Technology represent the Board on interactions with the Oversight Committee on Audit, IT Governance, Compliance and Accountability as appropriate to the topic.

### F. Meetings

Meetings are generally held at least once per academic quarter.

Meetings are open to UCLA visitors with prior notice unless called otherwise by the Chair. Non-UCLA visitors attend at the discretion of the Chair. All visitors will be introduced.

*Closed sessions.* In consultation with legal counsel, the Board may go into closed session for certain agenda items at the direction of the Chair, with only voting members present. The attendance of non-voting or other individuals during such sessions is at the direction of the Chair. Student members may be excluded from closed sessions where deemed appropriate by the Chair.

### G. Web site

The Board will maintain a web site for publishing meeting materials, meeting summaries and any relevant documentation used by the Board. Materials will be assumed open to the campus and public unless declared confidential, privileged or otherwise limited by the Chair or legal counsel.

### Some topics previously addressed

- Development of a campus privacy statement
- Implications of the UC Electronic Communications Policy, records retention, e-discovery, information requests from law enforcement, application of CALEA
- Privacy implications of the UC Climate Assessment on Learning, Living and Working
- Research involving network traffic
- Illegal file sharing: articulating a campus position on lawsuits and network traffic monitoring
- Implications of security: external assessment, network instrumentation, future threats
- Data protection: policies, Task Force Report on use of SSNs at California Universities

## UC San Diego Information Data Security and Privacy Council

The UCSD Information Data Security and Privacy Council<sup>15</sup> (ISPC) is advisory to the UCSD Chief Ethics and Compliance Officer, who chairs the UCSD Compliance, Audit, Risk, and Ethics Committee (CARE). The ISPC is needed to achieve a cohesive organizational structure aligning responsibility, authority and accountability for effective enterprise computer security and information privacy. Because state and federal privacy rules are complex, potential privacy and security breaches need to be evaluated promptly to avoid fines and to determine whether the facts about the breach meet the criteria for external notifications to consumers and government agencies.

A separate UC San Diego Health Sciences Privacy / Security Advisory Board has been established which will report to this Council. This Board will perform similar activities to those outlined in this Charter for the Health Sciences enterprise.

<b>Chair</b>	<ul style="list-style-type: none"> <li>• Interim Chief Information Security and Privacy Officer</li> </ul>
<b>Members</b>	<ul style="list-style-type: none"> <li>• Chief Information Security Officer, Health Sciences; and Medical Center Representative</li> <li>• Scripps Institution of Oceanography Representative</li> <li>• Resource Management &amp; Planning Representative</li> <li>• Chief Human Resources, Safety &amp; Risk Management Officer, UCSD Medical Center</li> <li>• Administrative Computing &amp; Telecommunications</li> <li>• School of Medicine Representative</li> <li>• Research Affairs Representative</li> <li>• Chief Compliance and Privacy Officer, Health Sciences</li> <li>• External &amp; Business Affairs Representative</li> <li>• Administrative Computing &amp; Telecommunications (consultant)</li> <li>• Academic Affairs Representative</li> <li>• UCSD General Counsel</li> <li>• Student Affairs Representative</li> </ul>

### Some topics previously discussed

Notification evaluation in potential breach situations

---

<sup>15</sup> [http://amas.ucsd.edu/Documents/04012010 ISPC Charter.pdf](http://amas.ucsd.edu/Documents/04012010%20ISPC%20Charter.pdf)

---

## INITIATIVE PARTICIPANTS

---

## Steering Committee

Chair	Glenn E. (Gene) Lucas, Santa Barbara Executive Vice Chancellor
Systemwide Representation and Support	Sheryl Vacca, Office of the President Senior Vice President and Chief Compliance and Audit Officer  David Ernst, Office of the President [-12/2012] Associate Vice President, Information Technology Services and Chief Information Officer
2 faculty members designated by the UC Academic Senate	Matthew Franklin, Davis Professor of Computer Science  Rafail Ostrovsky, Los Angeles Professor of Computer Science
1 privacy expert	Christine Borgman, Los Angeles [6/2011-] Professor and Presidential Chair, Information Studies
Vice Chancellor for Research	Charles Louis, Riverside Vice Chancellor
Vice Chancellor for Administration	John Meyer, Davis Vice Chancellor, Administrative and Resource Management
Vice Chancellor for Student Affairs	Harry LeGrande, Berkeley Vice Chancellor
Campus IT Representative	James Davis, Los Angeles Vice Provost, IT and Chief Academic Technology Officer Chair, UCLA Board on Privacy and Data Protection
Medical Center CIO	Mike Minear, Davis Health Services Chief Information Officer
University Librarian	Karen Butter, San Francisco University Librarian/Assistant Vice Chancellor
Medical Center Privacy Officer	Lee Giddings, San Diego Health Sciences Medical Director, Compliance and Privacy Program
General Counsel	Charles Robinson, Office of the President Vice President and General Counsel
Chair, Academic Senate	Daniel Simmons, Systemwide Academic Senate [-6/2011] Academic Senate Chair  Robert Anderson, Systemwide Academic Senate [7/2011-12/2011] Academic Senate Chair  Robert Powell, Systemwide Academic Senate [1/2012-] Academic Senate Vice Chair; Chair

UCOP Academic Affairs	Lawrence Pitts, Office of the President [-7/2012] Provost and Executive Vice President  Aimée Dorr, Office of the President [7/2012-] Provost and Executive Vice President
UCOP Business Operations	Nathan Brostrom, Office of the President Executive Vice President
President's Compliance Committee	Peter Taylor, Office of the President Chief Financial Officer
Communications	Lynn Tierney, Office of the President Associate Vice President
Systemwide Policy Director for Information Management and Technology	Stephen Lau, Office of the President Systemwide Policy Director
Systemwide Privacy Officer	Russell Opland, Office of the President [-6/2011] Systemwide Privacy Officer and HIPAA Privacy and Security Officer
UC Undergraduate Student	Olutwatobi Afolayan, Riverside [-6/2011] UC Student Association  Joshua Van Gelder, Santa Cruz [9/2011-] UC Student Association
UC Graduate Student	Jessica Smith, Berkeley UC Student Association
Council of University of California Staff Assemblies	Brian Gresham, Merced Chair Elect, CUCSA Assistant Director, Capital Planning and Space Management
Working Group Chair	Kent Wada, Los Angeles Director, Strategic IT Policy and Chief Privacy Officer

## Working Group

Chair	Kent Wada, Los Angeles Director, Strategic IT Policy and Chief Privacy Officer
UC Academic Senate Faculty Designate	David Steigmann, Berkeley [9/2011–] Professor of Mechanical Engineering UC Academic Senate Committee on Academic Freedom
Information Technology Policy and UC Electronic Communications Policy	Karen Eft, Berkeley [–4/2011] IT Policy Manager  Stephen Lau, Office of the President Systemwide Policy Director for Information Management and Technology  Janine Roeth, Santa Cruz Director, Client Services and Security and Information Security Officer
Information Technology Security	Jon Good, Office of the President Director, IT Security  Karl Heins, Santa Barbara [–9/2012] Chief Information Security Officer  Robert Ono, Davis IT Security Coordinator
Campus Privacy	Ann Geyer, Berkeley [5/2011–7/2012] Chief Privacy Officer
Medical Center Privacy	Martha (Marti) Arvin, UCLA Health System and David Geffen School of Medicine [6/2011–] Chief Compliance Officer and Systemwide Health Sciences Privacy Liaison  Kathleen Naughton, UC San Diego Health Sciences Chief Compliance and Privacy Officer
Systemwide Privacy Officer	Russell Opland, Office of the President [–6/2011] Systemwide Privacy Officer and HIPAA Privacy and Security Officer
Legal Counsel	Maria Shanle, Office of the General Counsel [–10/2011,3/2012–] Senior University Counsel  Cynthia Vroom, Office of the General Counsel [10/2011–3/2012] Senior University Counsel
Records Management Policies	Meta Clow, Santa Barbara Policy and Information Stewardship Officer
Graphics design and project support	Kelly Arruda, Los Angeles Project Manager

## Acknowledgements

### Insight

- UCLA Advisory Board on Privacy and Data Protection<sup>16</sup> for providing a basis for the UC Statement of Privacy Values
- UC Information Technology Policy and Security group<sup>17</sup> for development of the Report of the UC IT Policy and Security Workgroup
- UC Records and Information Management Committee<sup>18</sup> for development of a report on the intersections between privacy and records and information management.
- Daniel J. Solove, John Marshall Harlan Research Professor of Law at the George Washington University Law School
- Chris Jay Hoofnagle, Director of the Berkeley Center for Law & Technology's information privacy programs and senior fellow to the Samuelson Law, Technology & Public Policy Clinic
- Deirdre Mulligan, professor of law at the UC Berkeley School of Information and a Faculty Director of the Berkeley Center for Law and Technology
- Joanne McNabb, Chief, California Office of Privacy Protection

### Administrative support

- Paula Eeds, Information Technology Services, UCOP
- Joanne Fife, Office of Information Technology, UCLA

### Sources

1. Clarke, R. (2006). Introduction to Dataveillance and Information Privacy, and Definitions of Terms. <[rogerclarke.com/DV/Intro.html](http://rogerclarke.com/DV/Intro.html)>
2. Organisation of Economic Development. Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. <[oecd.org/document/18/0,3343,en\\_2649\\_34255\\_1815186\\_1\\_1\\_1\\_1,00.html](http://oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html)>
3. Federal Trade Commission. Fair Information Practice Principles. <[ftc.gov/reports/privacy3/fairinfo.shtm](http://ftc.gov/reports/privacy3/fairinfo.shtm)>
4. American Institute of CPAs et al. Generally Accepted Privacy Principles (GAPP). <[aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx](http://aicpa.org/InterestAreas/InformationTechnology/Resources/Privacy/GenerallyAcceptedPrivacyPrinciples/Pages/default.aspx)>
5. Solove, D. J. (2007). 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. *San Diego Law Review*, 44, 745-773. <[papers.ssrn.com/sol3/papers.cfm?abstract\\_id=998565](http://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565)>
6. Federal Trade Commission. (December 2010). Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Businesses and Policymakers. <<http://www.ftc.gov/os/2012/03/120326privacyreport.pdf>>

---

<sup>16</sup> <http://privacyboard.ucla.edu/>

<sup>17</sup> <http://www.ucop.edu/irc/itlc/itps/>

<sup>18</sup> <http://www.ucop.edu/irc/recman/>

## Glossary

**Autonomy privacy** An individual's ability to conduct activities without concern of or actual observation

**"Big Data"** Large aggregated data sets of information, which may include transactional information online such as web logs, social media information or searches

**Campus** Any UC location (e.g., campus, medical center, Office of the President) or Lawrence Berkeley National Lab

**Campus Privacy Program** A coordination of activities necessary to develop a unified culture of privacy consistent with the UC Statement of Privacy Values and Principles

**Electronic Communications Policy** The UC Electronic Communications Policy (ECP) establishes principles, rules and procedures applying to all members of the University community to specifically address issues particular to the use of electronic communications

**FERPA** The Family Educational Rights and Privacy Act is a Federal law that protects the privacy of student education records

**Governance** Oversees the principles and program, ensures compliance and provides high-level strategic direction (the "what")

**HIPAA** The Health Insurance Portability and Accountability Act of 1996, is a Federal law that, among other things, protects the privacy of individually identifiable health information

**Incidental personal use** A general concept, but as defined specifically by the ECP, the use of University resources for non-University activities, where "use does not: (i) interfere with the University's operation of electronic communications resources; (ii) interfere with the user's employment or other obligations to the University, or (iii) burden the University with noticeable incremental costs"

**Information privacy** The appropriate protection, use and dissemination of information about individuals. Information privacy protects data about people

**Information security** Supports the protection of information resources from unauthorized access, which could compromise the confidentiality, integrity, and availability of those resources. Information security protects data and infrastructure

**IS-3** UC Business and Finance Bulletin IS-3, Electronic Information Security

**Management** Directs and facilitates implementation of the campus privacy or information security program (the "how")

**Operations** Each unit must implement the program as appropriate, in accordance with management directives (drives toward the "what" with the "how")

**Privacy Balancing Process** A tool that applies the UC Privacy Values and Principles to adjudicate between competing values, obligations and interests of the University, intended for use by privacy boards, privacy officials and others both in making policy and to guide case-specific decision-making

**Privacy by design** In general, the philosophy of embedding privacy proactively; making it the default

**Records and information management** Policy, regulations and general principles for appropriately managing, accessing and preserving administrative records throughout their lifecycle and schedules for their final disposition

**UC Privacy Principles** Principles derived from the UC Statement of Privacy Values and intended to be used to guide policies and practice

**UC Statement of Privacy Values** Declares privacy—of both autonomy and information—as an important value of the University and clarifies that privacy is one of many values and obligations of the University