Privacy and Information Security Initiative Steering Committee Report to the President

Executive Summary

January 2013 | The University of California

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:

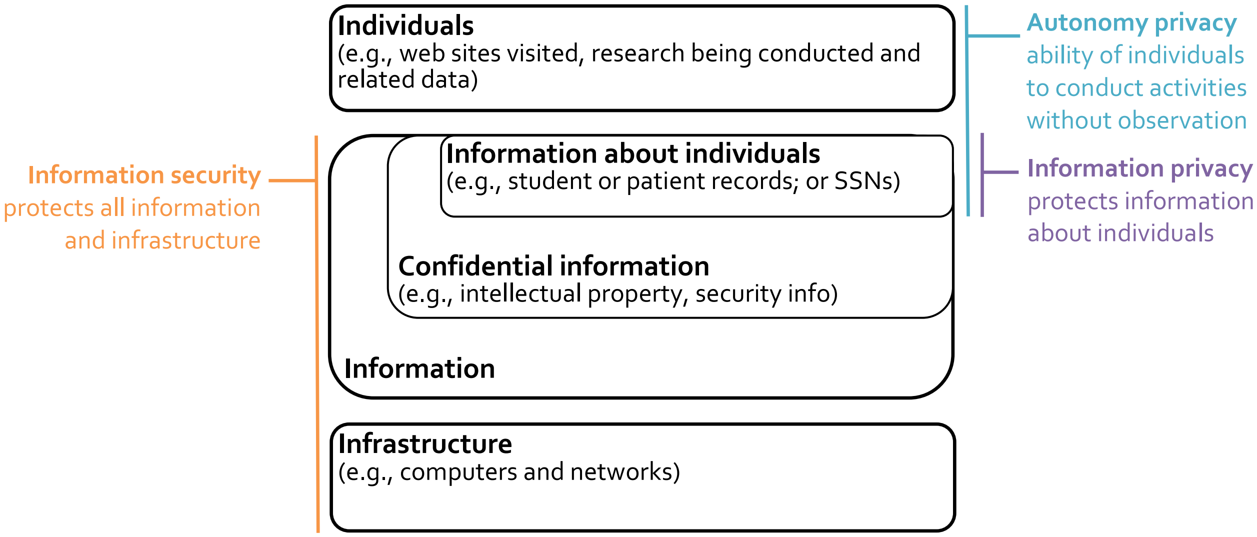
1. An overarching privacy framework that enables UC to meet statutory and regulatory obligations in a manner respectful of individual privacy;	All recommendations and Definitions (page **Error! Bookmark not defined.**)
2. Governance, implementation, and accountability structures across the University 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.


Individuals
(e.g., web sites visited, research being conducted and related data)
Autonomy privacy
ability of individuals to conduct activities without observation
Information security
protects all information and infrastructure
Information about individuals
(e.g., student or patient records; or SSNs)
Information privacy
protects information about individuals
Confidential information
(e.g., intellectual property, security info)
Information
Infrastructure
(e.g., computers and networks)

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.

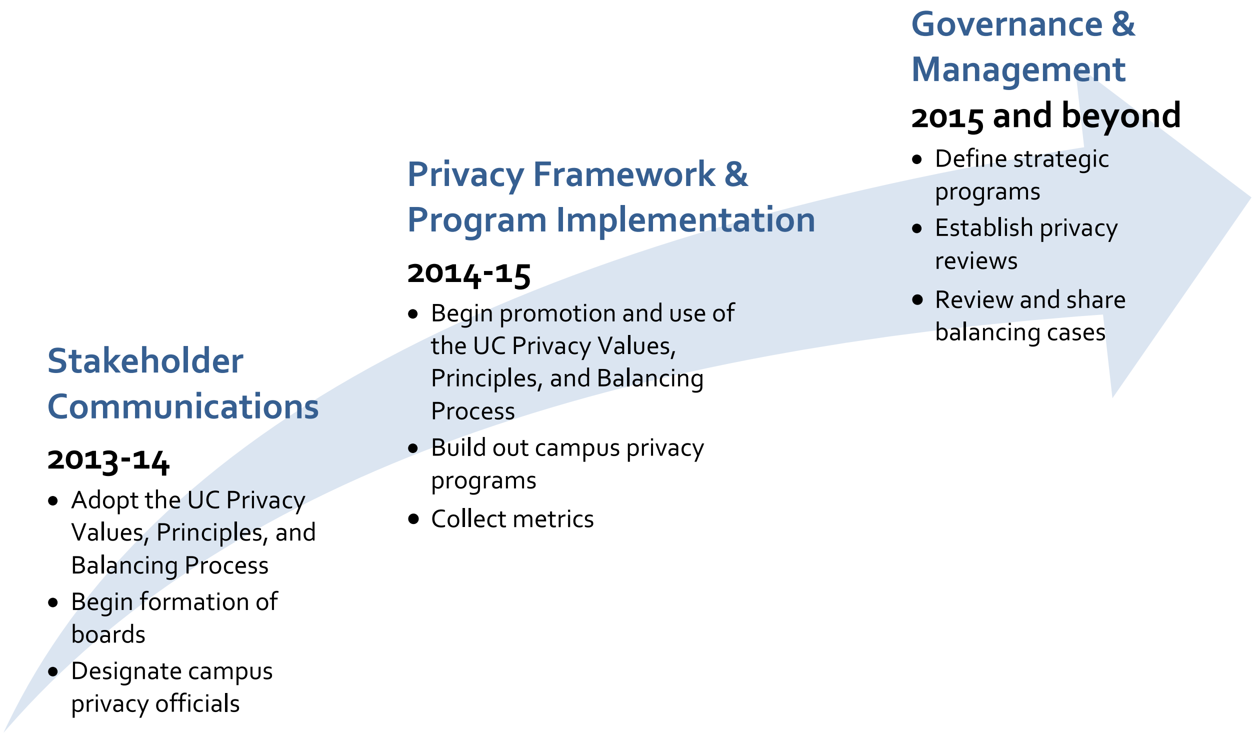
RECOMMENDATION 4: Campus Privacy Official. Each Chancellor should be charged with designating a privacy official to be responsible for the collaborative development, implementation, and administration of a unified privacy program for the campus. The privacy official shall work closely with the campus's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



Stakeholder Communications

2013-14

- Adopt the UC Privacy Values, Principles, and Balancing Process
- Begin formation of boards
- Designate campus privacy officials

Privacy Framework & Program Implementation

2014-15

- Begin promotion and use of the UC Privacy Values, Principles, and Balancing Process
- Build out campus privacy programs
- Collect metrics

Governance & Management

2015 and beyond

- Define strategic programs
- Establish privacy reviews
- Review and share balancing cases